

Part No. 215662-B  
December 2003

4655 Great America Parkway  
Santa Clara, CA 95054

# **Reference for the BayStack 420/425 Management Software, Software version 3.0**

**NORTEL**  
**NETWORKS™**

## Copyright © 2003 Nortel Networks

All rights reserved. December 2003.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

## Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and BayStack 425 are trademarks of Nortel Networks.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

SPARC is a trademark of Sparc International, Inc.

Sun and Solaris are trademarks of Sun Microsystems, Inc.

HP is a trademark of Hewlett-Packard Corporation.

UNIX is a trademark of X/Open Company Limited.

IBM and AIX are trademarks of International Business Machines Corporation (IBM).

Netscape Navigator is a trademark of Netscape Communications Corporation.

Ethernet is a trademark of Xerox Corporation.

Intel and Pentium are trademarks of Intel Corporation.

The asterisk after a name denotes a trademarked item.

## Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

## Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

## Nortel Networks Inc. software license agreement

**NOTICE:** Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

**1. License grant.** Nortel Networks Inc. (“Nortel Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

**2. Restrictions on use; reservation of rights.** The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

**3. Limited warranty.** Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER

WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

**4. Limitation of liability.** IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

**5. Government licensees.** This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

**6. Use of software in the European Community.** This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

**7. Term and termination.** This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

**8. Export and re-export.** Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

**9. General.** If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks Inc., 2375 N. Glenville Dr., Richardson, TX 75082.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

---

# Contents

---

<b>Preface</b> .....	<b>19</b>
Before you begin .....	19
Text conventions .....	19
Related publications .....	20
How to get help .....	21
 <b>Chapter 1</b>	
<b>Device Manager basics</b> .....	<b>23</b>
Starting Device Manager .....	23
Setting the Device Manager properties .....	24
Opening a device .....	27
Device Manager window .....	29
Menu bar .....	30
Toolbar .....	31
Device view .....	31
Selecting objects .....	32
Selecting a single object .....	32
Selecting multiple objects .....	33
LEDs and ports .....	34
Shortcut menus .....	35
Status bar .....	36
Using the buttons in Device Manager dialog boxes .....	37
Editing objects .....	38
Working with statistics and graphs .....	38
Types of statistics .....	39
Types of graphs .....	39
Statistics for single and multiple objects .....	42
Viewing statistics as graphs .....	43

Telneting to a switch .....	45
Opening the Web-based management home page .....	46
Trap log .....	47
Online Help .....	49

## **Chapter 2**

### **Configuring and graphing the switch ..... 51**

Viewing switch IP information .....	51
Globals tab .....	51
Addresses tab .....	52
ARP tab .....	53
Editing the chassis configuration .....	55
System tab .....	55
Base Unit Info tab .....	58
Stack Info tab .....	60
Agent tab .....	62
SNMP tab .....	64
Trap Receivers tab .....	65
Adding a Trap Receiver .....	66
Power Supply tab .....	67
Fan tab .....	69
Working with configuration files .....	70
ASCII config file .....	72
Graphing chassis statistics .....	74
SNMP tab .....	74
IP tab .....	77
ICMP In tab .....	80
ICMP Out tab .....	82

## **Chapter 3**

### **Configuring and graphing ports..... 85**

Viewing and editing a single port configuration .....	85
Interface tab for a single port .....	86
VLAN tab for a single port .....	88
STG tab for a single port .....	91

---

EAPOL tab for a single port .....	93
Viewing and editing multiple port configurations .....	95
Graphing multiple ports .....	97
Interface tab for multiple ports .....	97
VLAN tab for multiple ports .....	99
EAPOL tab for multiple ports .....	101
Graphing port statistics .....	103
Interface tab for graphing ports .....	104
Ethernet Errors tab for graphing ports .....	106
Bridge tab .....	110
RMON tab .....	111
EAPOL Stats tab for graphing ports .....	114
EAPOL Diag tab for graphing ports .....	116
 <b>Chapter 4</b>	
<b>Setting up MultiLink Trunk ports .....</b>	<b>117</b>
 MultiLink Trunk (MLT) features .....	117
Setting up MLTs .....	118
Adding ports to a MultiLink Trunk .....	119
MultiLink Trunk statistics .....	119
MultiLink Trunk Ethernet error statistics .....	121
 <b>Chapter 5</b>	
<b>Creating and managing VLANs .....</b>	<b>125</b>
 VLANs .....	125
Creating VLANs .....	126
VLAN Information .....	126
Creating a port-based VLAN .....	127
Accepting untagged frames .....	129
Modifying and managing existing VLANs .....	130
 <b>Chapter 6</b>	
<b>Setting up bridging .....</b>	<b>131</b>
 Base tab .....	131
Spanning Tree tab .....	132

---

Transparent tab .....	135
Forwarding tab .....	136
Spanning tree group (STG) .....	138
Configuration tab .....	139
Status tab .....	140
Ports tab .....	142
 <b>Chapter 7</b>	
<b>Troubleshooting Device Manager.....</b>	<b>145</b>
Topology tab .....	145
Topology Table tab .....	146
 <b>Chapter 8</b>	
<b>RMON .....</b>	<b>149</b>
Working with RMON information .....	149
Viewing statistics .....	149
Viewing history .....	150
Creating a history .....	152
Disabling history .....	154
Enabling Ethernet statistics gathering .....	155
Disabling Ethernet statistics gathering .....	156
Alarms .....	157
How RMON alarms work .....	157
Creating alarms .....	159
Alarm Manager example .....	160
Events .....	165
How events work .....	165
Viewing an event .....	165
Creating an event .....	167
Deleting an event .....	168
Log information .....	168
 <b>Chapter 9</b>	
<b>Security parameters.....</b>	<b>171</b>
General tab .....	171



---

SecurityList tab .....	174
Security, Insert SecurityList dialog box .....	175
AuthConfig tab .....	176
Security, Insert AuthConfig dialog box .....	177
AuthStatus tab .....	179
AuthViolation tab .....	181
SSH tab .....	183
SSH Sessions tab .....	184
<b>Index .....</b>	<b>187</b>



# Figures

---

Figure 1	Device Manager window	24
Figure 2	Properties dialog box	25
Figure 3	Open Device dialog box	28
Figure 4	Device view	29
Figure 5	Parts of the Device Manager window	30
Figure 6	Objects in the device view	32
Figure 7	Interface tab	34
Figure 8	Color port legend	35
Figure 9	Switch unit shortcut menu	35
Figure 10	Port shortcut menu	36
Figure 11	Line graph	40
Figure 12	Area graph	40
Figure 13	Bar graph	41
Figure 14	Pie graph	41
Figure 15	Interface statistics for a single port	42
Figure 16	Interface statistics for multiple ports	42
Figure 17	Statistics dialog box for a port	44
Figure 18	Open home page icon	46
Figure 19	Web-based management home page	47
Figure 20	Globals tab	52
Figure 21	Edit IP dialog box — IP Address tab	53
Figure 22	Edit IP dialog box — ARP tab	54
Figure 23	Edit Chassis dialog box — System tab	56
Figure 24	Edit Chassis dialog box — Base Unit Info tab	59
Figure 25	Edit Chassis dialog box — Stack Info tab	60
Figure 26	Edit Chassis dialog box — Agent tab	63
Figure 27	Edit Chassis dialog box — SNMP tab	64
Figure 28	Trap Receivers tab	65
Figure 29	Chassis, Insert Trap Receive dialog box	66

Figure 30	Edit Chassis dialog box — Power Supply tab . . . . .	68
Figure 31	Edit Chassis dialog box — Fan tab . . . . .	69
Figure 32	FileSystem - Config/Image/Diag File tab dialog box . . . . .	71
Figure 33	File system - ASCII Config File dialog box . . . . .	73
Figure 34	Graph Chassis dialog box — Chassis SNMP tab . . . . .	75
Figure 35	Graph Chassis dialog box — IP tab . . . . .	78
Figure 36	Graph Chassis dialog box — ICMP In tab . . . . .	81
Figure 37	Graph Chassis dialog box — ICMP Out tab . . . . .	82
Figure 38	Port dialog box — Interface tab . . . . .	86
Figure 39	Edit Port dialog box — VLAN tab . . . . .	89
Figure 40	Edit Port dialog box — STG tab . . . . .	91
Figure 41	Edit Port dialog box — EAPOL tab . . . . .	94
Figure 42	Graph Port dialog box — Interface tab . . . . .	98
Figure 43	VLAN tab for multiple ports . . . . .	100
Figure 44	EAPOL tab for multiple ports . . . . .	102
Figure 45	Interface tab for graphing ports . . . . .	104
Figure 46	Graph Port dialog box — Ethernet Errors tab . . . . .	107
Figure 47	Graph Port dialog box — Bridge tab . . . . .	110
Figure 48	Graph Port dialog box — RMON tab . . . . .	112
Figure 49	Graph Port dialog box — EAPOL Stats tab . . . . .	115
Figure 50	Graph Port dialog box — EAPOL Diag tab . . . . .	116
Figure 51	MLT dialog box . . . . .	118
Figure 52	PortMembers dialog box . . . . .	119
Figure 53	MLT Statistics — Interface tab . . . . .	120
Figure 54	MLT Statics dialog box — Ethernet Errors tab . . . . .	121
Figure 55	VLAN - Basic dialog box . . . . .	126
Figure 56	VLAN dialog box- Snoop tab . . . . .	127
Figure 57	VLAN, Insert Basic dialog box for a port-based VLANs . . . . .	128
Figure 58	VLAN tab . . . . .	129
Figure 59	VLAN dialog box . . . . .	130
Figure 60	Base tab . . . . .	132
Figure 61	Spanning Tree tab . . . . .	133
Figure 62	Transparent tab . . . . .	135
Figure 63	Forwarding tab . . . . .	137
Figure 64	Configuration tab . . . . .	139

---

Figure 65	Status tab .....	141
Figure 66	Ports tab .....	143
Figure 67	Diagnostics dialog box — Topology tab .....	145
Figure 68	Diagnostics dialog box — Topology Table tab .....	146
Figure 69	Port dialog box — RMON tab .....	150
Figure 70	Port dialog box — RMON tab .....	151
Figure 71	History tab .....	152
Figure 72	RMONControl, Insert History dialog box .....	153
Figure 73	RMONControl dialog box — Ether Stats tab .....	155
Figure 74	RMONControl, Insert Ether Stats dialog box .....	156
Figure 75	RMONControl, Insert Ether Stats dialog box port list .....	156
Figure 76	How alarms fire .....	158
Figure 77	Alarm example — threshold less than 260 .....	159
Figure 78	Alarm Manager dialog box .....	160
Figure 79	Alarm variable list .....	161
Figure 80	RMONAlarms dialog box — Alarms tab .....	163
Figure 81	RMONAlarms dialog box — Events tab .....	166
Figure 82	Insert Events dialog box .....	167
Figure 83	New event in the Events tab .....	167
Figure 84	Log tab .....	168
Figure 85	General tab .....	172
Figure 86	SecurityList tab .....	174
Figure 87	Security, Insert SecurityList dialog box .....	175
Figure 88	AuthConfig tab .....	176
Figure 89	Security, Insert AuthConfig dialog box .....	178
Figure 90	AuthStatus tab .....	180
Figure 91	AuthViolation tab .....	182
Figure 92	SSH tab .....	183
Figure 93	SSH Sessions tab .....	185



# Tables

---

Table 1	Properties dialog box items .....	26
Table 2	SNMP community string default values .....	27
Table 3	Open Device dialog box fields .....	28
Table 4	Menu bar commands .....	30
Table 5	Toolbar buttons .....	31
Table 6	Port color codes .....	34
Table 7	Switch unit shortcut menu command .....	36
Table 8	Port shortcut menu commands .....	36
Table 9	Device Manager buttons .....	37
Table 10	Types of statistics .....	39
Table 11	Graph dialog box buttons .....	45
Table 12	Help file locations .....	49
Table 13	Globals tab items .....	52
Table 14	IP Addresses tab items .....	53
Table 15	ARP tab items .....	54
Table 16	System tab items .....	56
Table 17	Base Unit Info tab items .....	59
Table 18	Stack Info tab fields .....	61
Table 19	Agent tab fields .....	63
Table 20	SNMP tab fields .....	65
Table 21	Edit Chassis dialog box — Trap Receivers tab items .....	66
Table 22	Power Supply tab fields .....	68
Table 23	Fan tab fields .....	70
Table 24	FileSystem Config/Image/Diag file dialog box items .....	71
Table 25	FileSystem - ASCII Config File dialog box items .....	73
Table 26	SNMP tab fields .....	75
Table 27	Chassis IP tab fields .....	78
Table 28	ICMP In tab fields .....	81
Table 29	ICMP Out tab fields .....	83

Table 30	Interface tab items for a single port . . . . .	87
Table 31	VLAN tab items for a single port . . . . .	89
Table 32	STG tab items for a single port . . . . .	92
Table 33	EAPOL tab items for a single port . . . . .	94
Table 34	Interface tab fields for multiple ports . . . . .	98
Table 35	VLAN tab fields for multiple ports . . . . .	100
Table 36	EAPOL tab fields for multiple ports . . . . .	102
Table 37	Port Interface tab fields for multiple ports . . . . .	105
Table 38	Ethernet Errors tab fields . . . . .	108
Table 39	Bridge tab fields . . . . .	111
Table 40	RMON tab fields . . . . .	112
Table 41	EAPOL tab fields . . . . .	115
Table 42	MLT dialog box fields . . . . .	118
Table 43	Interface tab fields . . . . .	120
Table 44	Ethernet Errors tab fields . . . . .	122
Table 45	VLAN dialog box fields . . . . .	126
Table 46	VLAN - Snoop dialog box fields . . . . .	127
Table 47	VLAN dialog box fields . . . . .	130
Table 48	Base tab fields . . . . .	132
Table 49	Spanning Tree tab fields . . . . .	133
Table 50	Transparent tab items . . . . .	136
Table 51	Forwarding tab fields . . . . .	138
Table 52	Configuration tab fields . . . . .	139
Table 53	Status tab fields . . . . .	141
Table 54	Ports tab fields . . . . .	143
Table 55	Topology tab items . . . . .	146
Table 56	Topology Table tab fields . . . . .	147
Table 57	History tab fields . . . . .	153
Table 58	Ether Stats tab fields . . . . .	155
Table 59	RMON Insert Alarm dialog box fields . . . . .	162
Table 60	Describes the fields on the Alarms tab . . . . .	163
Table 61	Events tab fields . . . . .	166
Table 62	Log tab fields . . . . .	169
Table 63	General tab items . . . . .	172
Table 64	SecurityList tab fields . . . . .	174



---

Table 65	Security, Insert AuthConfig dialog box fields . . . . .	175
Table 66	AuthConfig tab fields . . . . .	176
Table 67	Security, Insert AuthConfig dialog box fields . . . . .	178
Table 68	AuthStatus tab fields . . . . .	180
Table 69	AuthViolation tab fields . . . . .	182
Table 70	SSH tab fields . . . . .	183
Table 71	SSH Sessions tab fields . . . . .	185



---

# Preface

---

Welcome to the Nortel Networks\* Device Manager software, a set of graphical network management applications you can use to configure and manage the Nortel Networks BayStack\* 420/425 Switch. This guide provides information about using the features and capabilities of the Java-based Device Manager graphical user interface (GUI) to perform network management operations for the switch.



**Note:** This version of Device Manager supports BayStack 420/425 Switch software version 3.0.

---

## Before you begin

This guide is intended for network administrators with the following background:

- Basic knowledge of networks and Ethernet\* bridging
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies
- Familiarity with GUIs

## Text conventions

This guide uses the following text conventions:

*italic text*

Indicates book titles.

separator ( > )

Shows menu paths.

Example: Protocols > IP identifies the IP option on the Protocols menu.

## Related publications

For more information about using the BayStack 420/425 Switch, refer to the following publications:

- *Installing the BayStack 425 10/100/1000 Switch* (part number 215658-A)  
Describes how to install the BayStack 420/425 Switch.
- *Getting Started with BayStack 420/425 Software* (part number 215663-A)  
Describes how to install the Device Manager software management application.
- *Using the BayStack 425 10/100/1000 Switch* (part number 215661-A)  
Describes how to use the BayStack 420/425 Switch for network configuration.
- *Using Web-based Management for the BayStack 425 10/100/1000 Switch, Software Version 2.0* (part number 215660-A)  
Describes how to use the Web-based management tool to configure switch features.
- *Reference for the BayStack 425 Command Line Interface* (part number 215659-A)  
Describes how to use Command Line Interface (CLI) commands to configure and manage the BayStack 420/425 Switch.

You can print selected technical manuals and release notes free, directly from the Internet. Go to the [www.nortelnetworks.com/documentation](http://www.nortelnetworks.com/documentation) URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe\* Acrobat Reader\* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the [www.adobe.com](http://www.adobe.com) URL to download a free copy of the Adobe Acrobat Reader.

## How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000



---

# Chapter 1

## Device Manager basics

---

This chapter describes basic procedures for using the Device Manager software. The chapter includes the following information:

- Instructions to start Device Manager, set the Device Manager properties, and open a device (next)
- A summary of the Device Manager user interface features and how to use them (starting on [page 29](#))
- Instructions to view statistics and display graphs ([page 38](#))
- Instructions to use Device Manager to Telnet to a switch ([page 45](#))
- Information about the trap log ([page 47](#))
- Information about online Help ([page 49](#))



---

**Note:** This version of Device Manager supports BayStack 420/425 software version 3.0.

---

## Starting Device Manager

➡ Do one of the following, depending upon your operating system environment:

- In a Microsoft® Windows® environment, from the Windows taskbar choose Start > Programs > Java Device Manager Software > DM.
- In a UNIX environment, verify that the Device Manager installation directory is in your search path; then enter:

`./JDM`

The initial Device Manager window opens ([Figure 1](#)).



**Note:** On startup, Device Manager performs a DNS lookup for the machine on which it is running. If the DNS lookup is slow or fails, the initial Device Manager window may take up to 30 seconds to open.

---

**Figure 1** Device Manager window



## Setting the Device Manager properties

Device Manager communicates with the BayStack 420/425 switch using Simple Network Management Protocol (SNMP). The software is shipped with default values set for important communication parameters, such as the polling interval, timeout, and retry count. You may want to set the parameters before you open a device to manage.

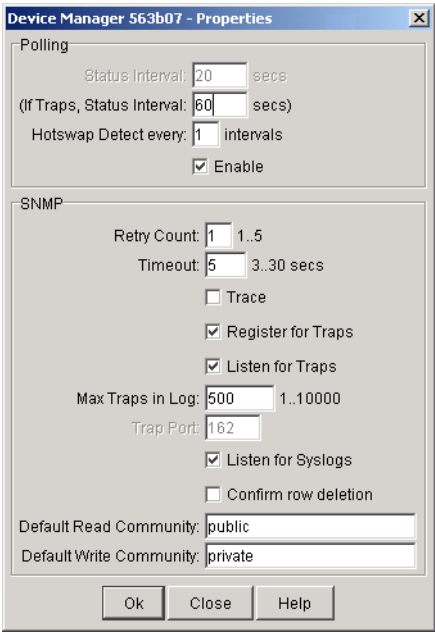
To set the Device Manager properties:

- 1 Choose Device > Properties.

The Properties dialog box opens ([Figure 2](#)).



**Figure 2** Properties dialog box



- 2 Type information and select check boxes.
- 3 Click OK.

Table 1 describes the Properties dialog box items.

**Table 1** Properties dialog box items

Area	Item	Description
<b>Polling</b>	Status Interval	Interval at which status information is gathered (default is 20 seconds). For a full stack, set this interval to 60 seconds.
	(If Traps, Status Interval: )	Interval at which statistics and status information are gathered when traps are enabled. The default is 60.
	Hotswap Poll Interval	The interval at which Device Manager polls for module information. The default is 1 interval.
	Enable	Enables (true) or disables (false) periodic polling of the device for updated status. If polling is disabled, the chassis status is updated only when you click Refresh on the Chassis tab.
<b>SNMP</b>	Retry Count	Number of times Device Manager sends the same polling request if a response is not returned to Device Manager. You may want to set this field to three or four.
	Timeout	Length of each retry of each polling waiting period. When you access the device through a slow link, you may want to increase the timeout interval and then change the Retransmission Strategy to superlinear.
	Trace	The trace field is used to enable and disable SNMP tracing. When Trace is selected, SNMP protocol data units (PDUs) are displayed in the Device > Log dialog box.
	Register for Traps	When selected (enabled), automatically registers to received traps when Device Manager is launched against a device.
	Max Traps in Log	The specified number of traps that may exist in the trap log. The default is 500.
	Trap Port	Specifies the UDP port that Device Manager will listen to receive SNMP traps.
	Listen for Syslogs	Specifies listening to system logs.
	Confirm row deletion	A dialog box displays when checked, before deleting a row.
	Default read community	Specifies the default read community.
	Default write community	Specifies the default write community.

## Opening a device

“Opening” a device displays the device view, a picture of the device. To open the device view, you must enter community strings that determine the access level granted to the device.

[Table 2](#) shows the default access community strings for the Device Manager software.

**Table 2** SNMP community string default values

Access level	Description
Read-only	public
Read/write	private

To display the device view:

**1** Do one of the following:

- Choose Device > Open.
- Choose Device > Open Last, and select an IP address from the list.
- Click the folder icon in the Device Manager window.



- Press [Ctrl] + O.

The Open Device dialog box opens ([Figure 3](#)).

**Figure 3** Open Device dialog box

Table 3 describes the Open Device dialog box fields.

**Table 3** Open Device dialog box fields

Field	Description
Device Name	Either an IP address or a DNS name for the device, entered by the user.
Read Community	SNMP read community string for the device. Default is <code>public</code> (displayed as <code>*****</code> ). The entry is case-sensitive.
Write Community	SNMP write community string for the device. Default is <code>private</code> (displayed as <code>*****</code> ). The entry is case-sensitive.

- 2 In the Device Name text box, type the DNS name or IP address of the device.
- 3 In the Read Community and Write Community text boxes, type the proper community strings.



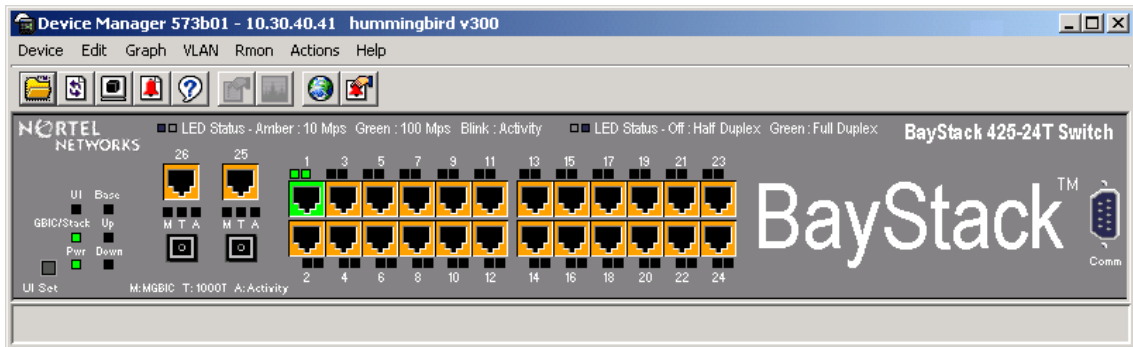
**Note:** To gain read/write access to a device in Device Manager, you must enter the read/write community string for both the Read Community and Write Community strings.

#### 4 Click Open.

Device Manager automatically determines what version of software the selected device is running and displays the appropriate Device Manager dialog boxes.

The Device Manager window opens, showing a picture of the device (Figure 4) that represents the physical features of the device.

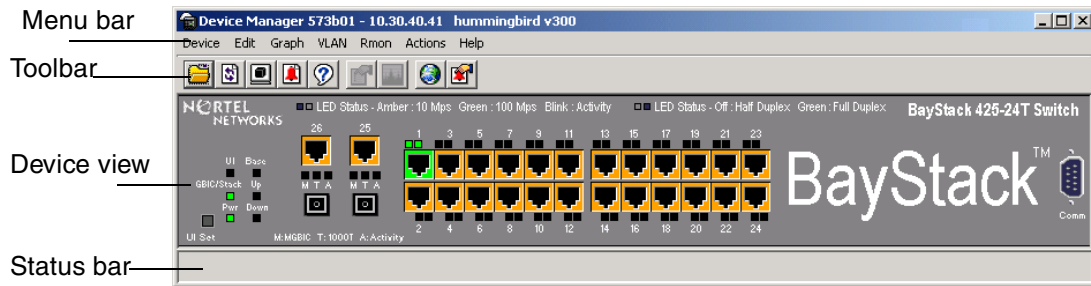
**Figure 4** Device view



## Device Manager window

The Device Manager window (Figure 5) has the following parts:

- Menu bar
- Toolbar
- Device view
- Status bar

**Figure 5** Parts of the Device Manager window

## Menu bar

Use the menu bar to set up and operate Device Manager ([Table 4](#)).










**Table 4** Menu bar commands

Command	Description
Device	Opens the Open Device dialog box.
Edit	Opens edit dialog boxes for selected objects in the device view. This command also opens dialog boxes for managing files and running diagnostic tests.
Graph	Opens statistics dialog boxes for the selected object.
VLAN	Opens dialog boxes for managing VLANs, spanning tree groups (STGs), and Multi-Link Trunks.
Rmon	Opens RMON configuration and monitoring dialog boxes.
Actions	Provides quick opening of a Telnet session without going through other dialog boxes. It also provides quick opening of the Web Management Software Home page.
Help	Opens online Help topics for Device Manager and provides a legend for the port colors in the device view.

## Toolbar

The toolbar contains buttons that provide quick access to commonly used commands and some additional actions.

**Table 5** Toolbar buttons

Button	Name	Description	Menu bar equivalent
	Open Device	Opens the Open Device dialog box.	Device > Open
	Refresh Device Status	Refreshes the device view information.	Device > Refresh Status
	Trap Log	Opens the trap log.	Device > Trap Log
	Help	Opens online Help in a Web browser.	Help > Device
	Edit Selected	Displays configuration data for the selected chassis object.	Edit > Unit Edit > Chassis Edit > Port
	Graph Selected	Opens statistics and graphing dialog boxes for the selected object.	Graph > Chassis Graph > Port
	Home Page	Opens the Web Management Software Home Page.	Actions > Open Home Page
	Telnet	Opens a Telnet session.	Device > Telnet
	Alarm Manager	Opens the Rmon Alarm Manager.	Rmon > Alarm Manager

## Device view

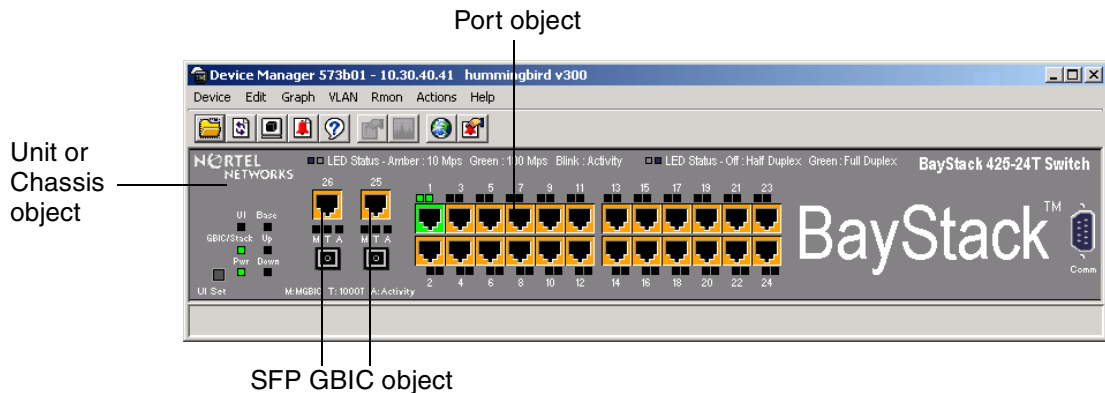
The device view allows you to determine at a glance the operating status of the various units and ports in your hardware configuration. You also use the device view to perform management tasks on specific objects.

## Selecting objects

The types of objects contained in the device view are:

- A standalone switch (called a unit in the menus and dialog boxes)
- A switch stack (called a chassis in the menus and dialog boxes)
- A port (including the SFP GBIC port)

**Figure 6** Objects in the device view



## Selecting a single object

To select a single object:

- ➡ Click the edge of the object.

The object is outlined in yellow, indicating that it is selected. Subsequent activities in Device Manager refer to the selected object.



## Selecting multiple objects

To select multiple objects of the same type (such as ports or switches of the same type):

➡ Do one of the following:

- For a block of contiguous ports, drag to select the group of ports.
- For multiple ports, GBICs, or switches in the stack, [Ctrl]-click on the objects.

To select all the ports in a standalone switch or in a switch stack:

➡ Choose Edit > Select > Ports.

To select all the units in the stack:

➡ Choose Edit > Select > Units.

To select an entire stack:

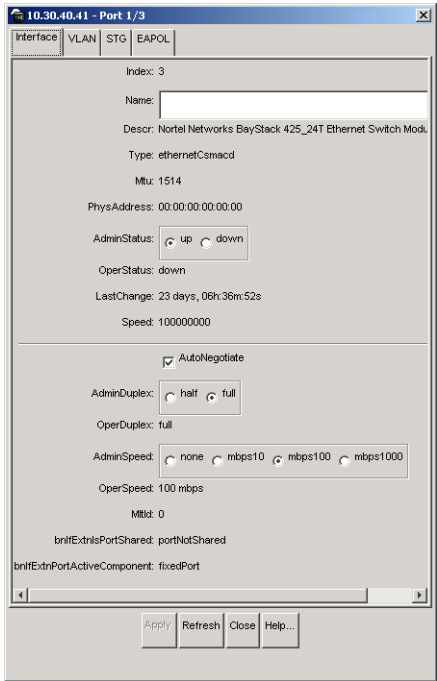
➡ Choose Edit > Select > Chassis.

To view information about a GBIC port:

- 1 Select the GBIC.
- 2 Choose Edit > Port.

The Port dialog box opens with the Interface tab displayed ([Figure 7](#)).  
The Interface tab describes the GBIC installed in the switch.

**Figure 7** Interface tab



**LEDs and ports**

The color of LEDs in the device view is the same as the colors of the LEDs on the physical switch. However, the device view does not show blinking activity of the LEDs.

For a full description of the LEDs for the Baystack 420/425, refer to *Using the BayStack 425 10/100 Switch*.

The ports on the device view are color coded to show port status.

Table 6 shows the status assigned to each color.

**Table 6** Port color codes

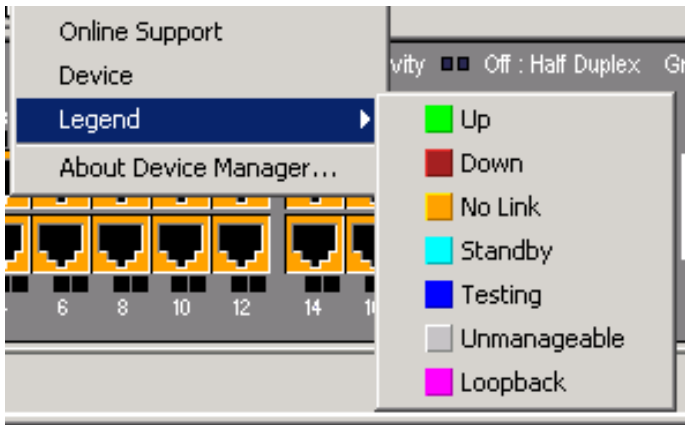
Color	Description
Green	Port is operating.

**Table 6** Port color codes (continued)

Color	Description
Red	Port has been manually disabled.
Orange	Port has no link.

In addition, the Help menu provides a legend that identifies the port colors and their meanings.

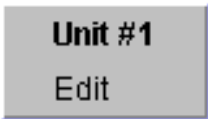
**Figure 8** Color port legend



## Shortcut menus

Each object in the device view has a shortcut menu that opens when you right-click a selected object. The switch unit shortcut menu ([Figure 9](#)) provides access to basic hardware information about the switch and to the graphing dialog boxes for the switch.

**Figure 9** Switch unit shortcut menu



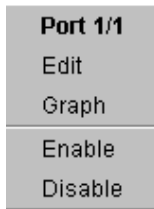
[Table 7](#) describes the Edit command on the switch unit shortcut menu.

**Table 7** Switch unit shortcut menu command

Command	Description
Edit	Opens a read-only dialog box that provides basic hardware information about the switch.

The port shortcut menu ([Figure 10](#)) provides a faster path for editing and graphing a single port; however, you can access the same options using the menu bar or the toolbar.

**Figure 10** Port shortcut menu



[Table 8](#) describes the commands on the port shortcut menu.

**Table 8** Port shortcut menu commands

Command	Description
Edit	Opens a dialog box that allows you to set operating parameters for the port.
Graph	Opens a dialog box that displays statistics for the port and allows you to display the statistics as a graph.
Enable	Administratively brings a port up.
Disable	Administratively shuts down a port. The color of the port changes to red in the device view.








## Status bar

The status bar displays error and informational messages from the software application. These messages are not related to the device being managed.

## Using the buttons in Device Manager dialog boxes

Table 9 describes buttons in Device Manager dialog boxes. Not all buttons appear in all dialog boxes.

**Table 9** Device Manager buttons

Button	Name	Description
	Insert	Opens a dialog box to create a new entry for a table; then from the dialog box, inserts the new entry in the table.
	Copy	Copies selected cells from a table.
	Paste	Pastes copied values to a currently selected table cell.
	Reset Changes	Causes changed (but not applied) fields to revert to their previous values.
	Print Table or Print Graph	Prints the table or graph that is displayed.
	Stop/Refresh	Stops the current action (compiling, saving, and so forth). If you are updating or compiling a large data table, the Refresh button changes to a Stop button while this action is taking place. Clicking the Stop button interrupts the polling process.
	Export Data	Exports information to a file you specify. You can then import this file into a text editor or spreadsheet for further analysis.

## Editing objects

You can edit objects and values in the Device Manager device view in the following ways:

- Select an object and, on the toolbar, click the Edit Selected button.



The edit dialog box opens for that object.

- From a switch or port shortcut menu, choose Edit. The edit dialog box opens for that object.

When you change the value in a box, the changed value is displayed in **bold**. However, changes are not applied to the running configuration until you click Apply.



**Note:** Many dialog boxes contain a Refresh button. After you apply changes to fields, click Refresh to display the new information in the dialog box.

---

## Working with statistics and graphs

Device Manager tracks a wide range of statistics for the stack (chassis), and each port. You can view and graph statistics for a single object or multiple objects. For information about the statistics tracked for the switch and ports, refer to [“Statistics for single and multiple objects” on page 42](#) and [“Graphing chassis statistics” on page 74](#).

This section describes the types of statistics and graphs available, the graph dialog boxes, and the procedure for creating a graph.

## Types of statistics

The data tables in the statistics dialog boxes list the counters, or categories of statistics being gathered, for the specified object. For example, the categories for ports include Interface, Ethernet Errors, Bridge, and Rmon. Each category can be associated with six types of statistics. [Table 10](#) describes the types of statistics that are available.

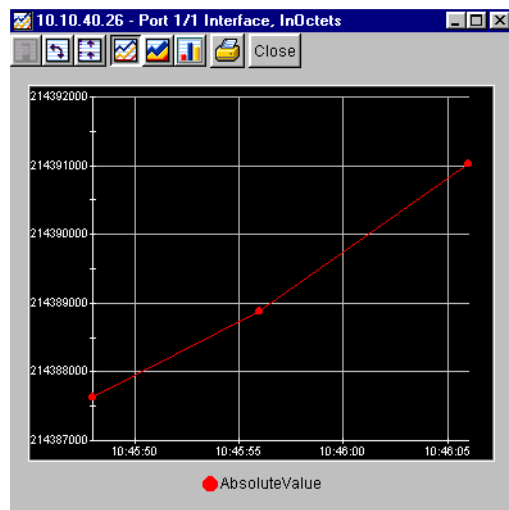
**Table 10** Types of statistics

Statistic	Description
AbsoluteValue	The total count since the last time counters were reset. A system reboot resets all counters.
Cumulative	The total count since the statistics window was first opened. The elapsed time for the cumulative counter is displayed at the bottom of the graph window.
Average	The cumulative count divided by the cumulative elapsed time.
Minimum	The minimum average for the counter for a given polling interval over the cumulative elapsed time.
Maximum	The maximum average for the counter for a given polling interval over the cumulative elapsed time.
LastValue	The average for the counter over the last polling interval.

## Types of graphs

With Device Manager, you can create line, area, bar, and pie graphs. [Figure 11](#), [Figure 12](#), [Figure 13](#), and [Figure 14](#) provide examples of different types of graphs.

**Figure 11** Line graph



**Figure 12** Area graph

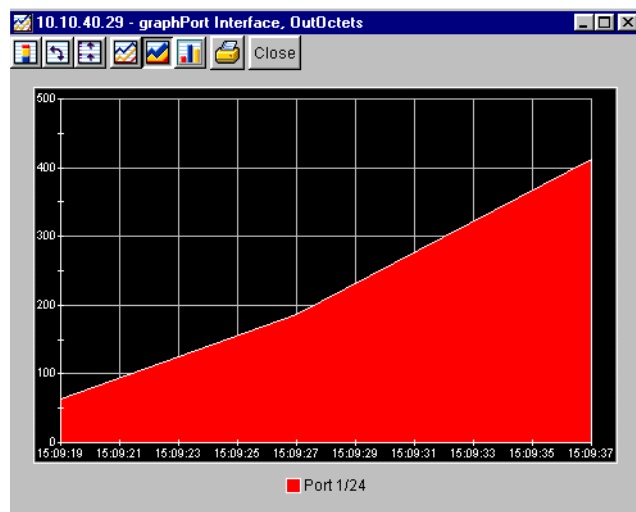




Figure 13 Bar graph

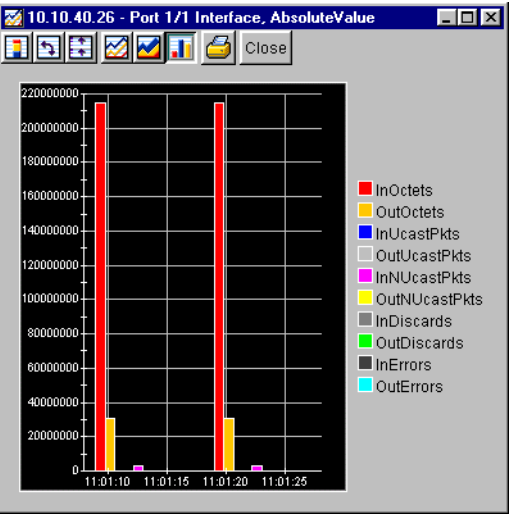
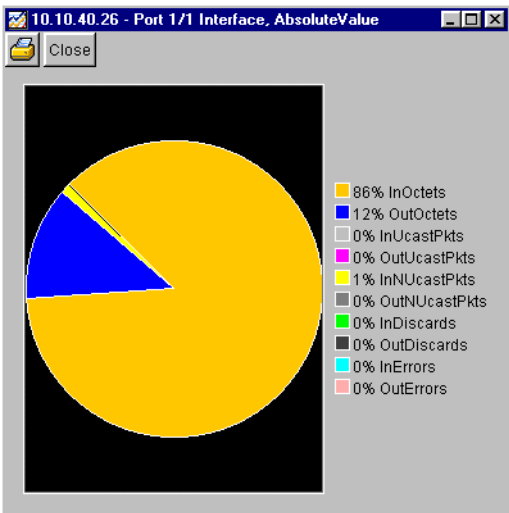


Figure 14 Pie graph

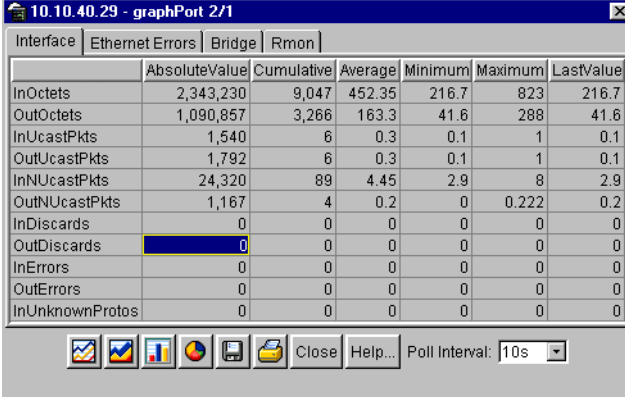


## Statistics for single and multiple objects

Statistics for a selected object or objects are displayed in the statistics dialog box.

The dialog box for a single object shows all six types of statistics for each counter (Figure 15).

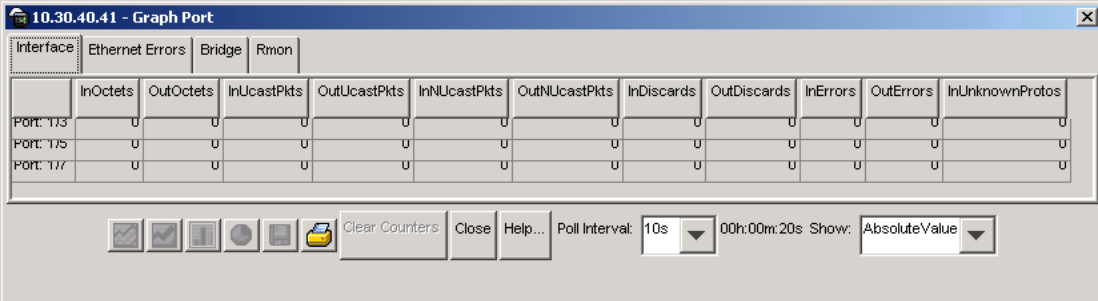
**Figure 15** Interface statistics for a single port



	AbsoluteValue	Cumulative	Average	Minimum	Maximum	LastValue
InOctets	2,343,230	9,047	452.35	216.7	823	216.7
OutOctets	1,090,857	3,266	163.3	41.6	288	41.6
InUcastPkts	1,540	6	0.3	0.1	1	0.1
OutUcastPkts	1,792	6	0.3	0.1	1	0.1
InNUcastPkts	24,320	89	4.45	2.9	8	2.9
OutNUcastPkts	1,167	4	0.2	0	0.222	0.2
InDiscards	0	0	0	0	0	0
OutDiscards	0	0	0	0	0	0
InErrors	0	0	0	0	0	0
OutErrors	0	0	0	0	0	0
InUnknownProtos	0	0	0	0	0	0

The statistics dialog box for multiple objects shows a single type of statistics (Table 10 on page 39) for the selected objects. For example, Figure 16 shows LastValue statistics for the selected ports.

**Figure 16** Interface statistics for multiple ports



	InOctets	OutOctets	InUcastPkts	OutUcastPkts	InNUcastPkts	OutNUcastPkts	InDiscards	OutDiscards	InErrors	OutErrors	InUnknownProtos
PORT: 173	0	0	0	0	0	0	0	0	0	0	0
PORT: 175	0	0	0	0	0	0	0	0	0	0	0
PORT: 177	0	0	0	0	0	0	0	0	0	0	0

To change the type of statistics displayed, select a different type from the show list at the bottom of the dialog box.

The statistics are updated based on the poll interval shown at the bottom of the dialog box. You can select a different polling interval.

Buttons for bar, pie, and line graphs are located at the bottom of a statistics dialog box.

See the next section, [“Viewing statistics as graphs,”](#) for instructions to use these buttons.

You can export the statistics to a tab-separated file format and import the file into other applications. To export the information, use the Export Data button below the table.



## Viewing statistics as graphs

To create a graph for an object:

- 1 Select the object or objects to be graphed.

See [“Selecting objects” on page 32.](#)

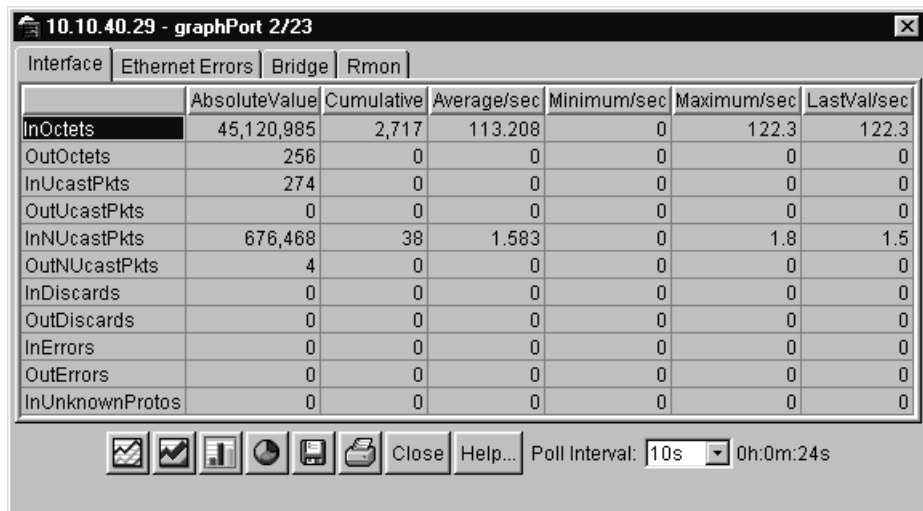
- 2 Do one of the following:

- On the toolbar, click Graph Selected.



- From the shortcut menu for the object, choose Graph.
- From the main menu, choose Graph > Chassis or Graph > Port.

A statistics dialog box opens with tabs for different categories of statistics for the selected object ([Figure 17](#)).

**Figure 17** Statistics dialog box for a port

- 3 Select a tab for the group of statistics you want to view.
- 4 On the displayed data table, drag to select the cells you want to graph. (They must be in the same row or column.)
- 5 Click one of the graph buttons at the bottom of the dialog box  
See [“Types of graphs” on page 39](#).

A graph dialog box opens for the selected graph type.







- 6 To print a copy of the graph, click Print.



Buttons at the top of the graph dialog boxes for line, area, and bar graphs allow you to change the orientation of the graph, change the scale, or change the graph type.

Table 11 describes the buttons in the graph dialog boxes.

**Table 11** Graph dialog box buttons

Button	Name	Description
	Stacked	“Stacks” data quantities instead of displaying them side-by-side.
	Horizontal	Rotates the graph 90 degrees.
	Log Scale	Changes the scale of the x-axis (of an unrotated graph) from numeric to logarithmic.
	Line Chart	Converts an area graph or bar graph to a line graph.
	Area Chart	Converts a line graph or bar graph to an area graph.
	Bar Chart	Converts a line graph or area graph to a bar graph.

## Telneting to a switch

From Device Manager, you can initiate a Telnet session to the console interface for the switch or stack you are currently accessing.

To Telnet to a switch:

➡ Do one of the following:

- From the Device Manager main menu, choose Device> Telnet.
- On the toolbar, click the Telnet button.



A Telnet window to the switch opens.

## Opening the Web-based management home page

From Device Manager, you can access the Web-based management home page.

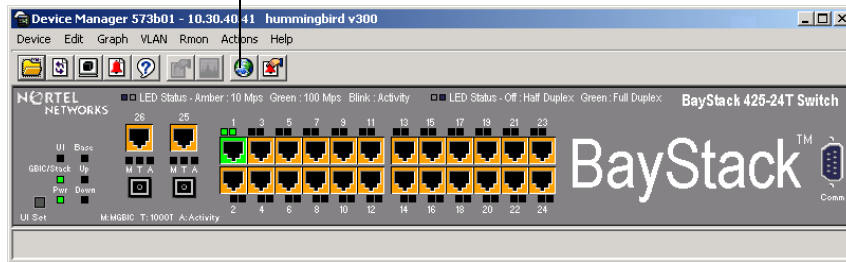
To open the Web-based management home page:

➡ Do one of the following:

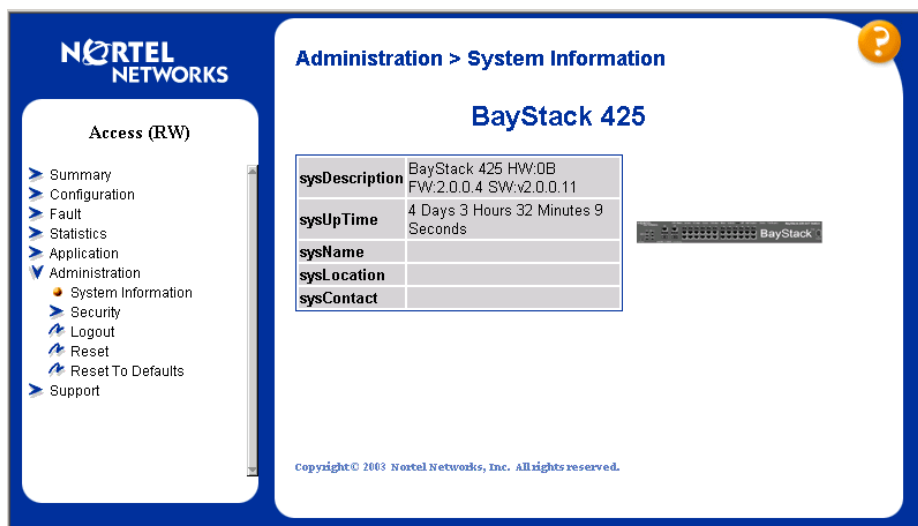
- From the Device Manager main menu, choose Actions > Open home page.
- On the toolbar, click the Open home page button.

**Figure 18** Open home page icon

Open Home Page



The Web-based management home page opens (Figure 19).

**Figure 19** Web-based management home page

## Trap log

You can configure a BayStack 420/425 Switch to send SNMP generic traps. When Device Manager is running, any traps received are recorded in the trap log. You set the maximum number of entries in the trap log using the Properties dialog box (Figure 2 on page 25). The default number of trap log entries is 500.

To view the trap log:

➡ Do one of the following:

- On the toolbar, click the Trap Log button.



- From the Device Manager Main Menu, choose Device > Trap Log.



**Note:** When you operate Device Manager from a UNIX platform, you must be logged in as root in order to receive traps.

Device Manager receives traps on port 162. If this port is being used by another application, you will not be able to view the trap log until the other application is disabled and Device Manager is restarted.

By default, traps are sent in SNMP V2c format. However, if you are using an older network management system (NMS), one that supports only SNMP V1 traps (HP OpenView), you can specify that the traps be sent in V1 format.

For more information about traps and trap receivers, refer to *Using the BayStack 425 10/100/1000 Switch*.



# Online Help

Online Help in Device Manager is context-sensitive. You use a Web browser to display online Help. The Web browser should launch automatically when you click the Help button. If the Help topic you are accessing is not displayed in your browser, exit the existing browser session and click the Help button again.

If, for some reason, the Web browser does not launch, the default locations of the Help files are the directories listed in [Table 12](#).

**Table 12** Help file locations

Platform	Default path
Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP	JDM install directory\help\hummingbird\v300\help.html
UNIX	JDM install directory\help\hummingbird\v300\help.html



---

## Chapter 2

# Configuring and graphing the switch

---

The first three sections of this chapter describe how you can use Device Manager to configure your switch. The last section describes how to use Device Manager to graph switch statistics.

## Viewing switch IP information

You can view the switch IP information using the IP dialog box.

To open the IP dialog box:

- From the Device Manager main menu, choose Edit > IP.

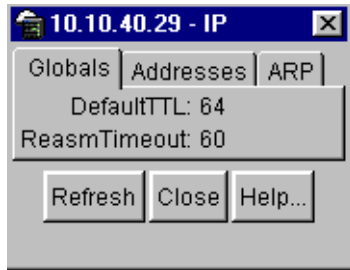
The Edit IP dialog box opens ([Figure 20 on page 52](#)) with the Globals tab displayed.

### Globals tab

To open the Globals tab:

- From the Device Manager main menu, choose Edit > IP.

The IP dialog box opens ([Figure 20](#)) with the Globals tab displayed.

**Figure 20** Globals tab

[Table 13](#) describes the Globals tab items.

**Table 13** Globals tab items

Item and MIB association	Description
DefaultTTL	Default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol. Default value is 16.
ReasmTimeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity. Default value is 5.

## Addresses tab

The Addresses tab shows the IP address information for the device.

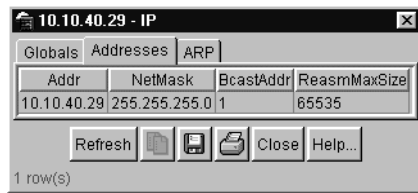
To open the Addresses tab:

- 1 From the Device Manager main menu, choose Edit > IP.

The IP dialog box opens with the Globals tab displayed ([Figure 20 on page 52](#)).

- 2 Click the Addresses tab.

The Addresses tab opens ([Figure 21 on page 53](#)).

**Figure 21** Edit IP dialog box — IP Address tab

[Table 14](#) describes the IP Address tab items.

**Table 14** IP Addresses tab items

Item	Description
Addr	The device IP address.
NetMask	The subnet mask address.
BcastAddr	The IP broadcast address used.
ReasmMaxSize	The size of the largest IP datagram that this entity can reassemble from incoming IP fragmented datagrams received on this interface.

## ARP tab

The Address Resolution Protocol (ARP) tab shows the MAC addresses and the associated IP addresses for the switch.

To open the ARP tab:

- 1 From the Device Manager main menu, choose Edit > IP.

The IP dialog box opens with the Globals tab displayed ([Figure 20 on page 52](#)).

- 2 Click the ARP tab.

The ARP tab opens ([Figure 22 on page 54](#)).

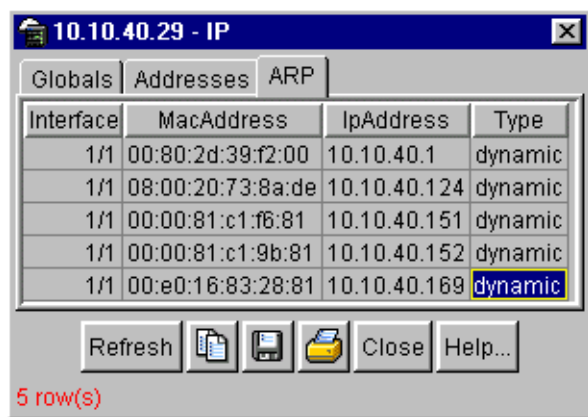
**Figure 22** Edit IP dialog box — ARP tab

Table 15 describes the ARP tab items.

**Table 15** ARP tab items

Item	Description
Interface	The device unit number.
MacAddress	The unique hardware address of the device.
IpAddress	The Internet Protocol address of the device used to represent a point of attachment in a TCP/IP internetwork.
Type	The type of mapping.

## Editing the chassis configuration

You can edit a chassis configuration from the Edit Chassis dialog box ([Figure 23 on page 56](#)).

To open the Chassis dialog box:

- 1** Select the chassis.
- 2** Do *one* of the following:
  - From the shortcut menu, choose Edit.
  - From the Device Manager main menu, choose Edit > Chassis.
  - On the toolbar, click Edit.



The following sections provide a description of the tabs in the Edit > Chassis dialog box and details about each item on the tab.

### System tab

You can use the System tab to specify, among other things, tracking information for a device and device descriptions.

To open the System tab:

- 1** Select the chassis.
- 2** From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens with the System tab displayed ([Figure 23](#)).

**Figure 23** Edit Chassis dialog box — System tab

The screenshot shows the 'Edit Chassis' dialog box with the 'System' tab selected. The dialog has a title bar '10.10.54.25 - Chassis' and several tabs: System, Base Unit Info, Stack Info, Agent, SNMP, Trap Receivers, PowerSupply, and Fan. The 'System' tab contains the following fields and controls:

- sysDescr:** BayStack 425 HW:0B FW:3.0.0.2 SW:v3.0.0.43
- sysUpTime:** 3 days, 00h:30m:27s
- sysContact:** (empty text field)
- sysName:** Hummingbird v300 (mix)
- sysLocation:** (empty text field)
- AuthenticationTraps:** ☒ (checked)
- ReBoot:** ☒ running ☐ reboot
- AutoPvid:** ☐ enabled ☒ disabled
- NextBootMgmtProtocol:** ipOnly
- CurrentMgmtProtocol:** ipOnly
- BootMode:** local
- ImageLoadMode:** net
- CurrentImageVersion:** v3.0.0.43
- LocalStorageImageVersion:** v3.0.0.43
- NextBootDefaultGateway:** 10.10.54.1
- CurrentDefaultGateway:** 10.10.54.1
- NextBootLoadProtocol:** ipOnly
- LastLoadProtocol:** ip
- EAPOL Security:**
  - SystemAuthControl:** ☐ enabled ☒ disabled

At the bottom of the dialog are four buttons: Apply, Refresh, Close, and Help...


Table 16 describes the System tab items.

**Table 16** System tab items

Item	Description
sysDescr	The assigned system name.
sysUpTime	The time since the system was last booted.
sysContact	Type the contact information (in this case, an e-mail address) for the system administrator.
sysName	Type the name of this device.
sysLocation	Type the physical location of this device.



**Table 16** System tab items (continued)

Item	Description
AuthenticationTraps	<p>Click enable or disable. When you select enabled, SNMP traps are sent to trap receivers for all SNMP access authentication. When you select disabled, no traps are received.</p> <p>To view traps, click the Trap toolbar button.</p> 
AutoPVID	Click enable or disable. When you select enabled, AutoPVID is activated. When you select disabled, AutoPVID is no longer active.
NextBootMgmtProtocol	The transport protocol(s) to use after the next boot of the agent.
CurrentMgmtProtocol	The current transport protocol(s) that the agent supports.
BootMode	The source from which to load the initial protocol configuration information to boot the switch the next time, local (from the switch), or net (over the network), or none.
ImageLoadMode	The source from which to load the agent image at the next boot.
CurrentImageVersion	The version number of the agent image that is currently used on the switch.
LocalStorageImageVersion	The version number of the agent image that is stored in flash memory on the switch.
NextBootDefaultGateway	The IP address of the default gateway for the agent to use after the next time the switch is booted.
CurrentDefaultGateway	The IP address of the default gateway that is currently in use.

**Table 16** System tab items (continued)

Item	Description
NextBootLoadProtocol	The transport protocol to be used by the agent to load the configuration information and the image at the next boot.
LastLoadProtocol	The transport protocol last used to load the image and configuration information on the switch.
Reboot	Action object to reboot the agent. Reboot — initiates a hardware reset. The agent does best efforts to return a response before the action occurs. If any of the combined download actions are requested, neither action occurs until the expiration of s5AgInfoScheduleBootTime, if set.
SystemAuthControl (enabled or disabled)	Specifies the administrative enabled or disable state for Port Access Control.

## Base Unit Info tab

The Base Unit Info tab provides read-only information about the operating status of the hardware and whether or not the default factory settings are being used.

To open the Base Unit Info tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens with the System tab displayed ([Figure 23 on page 56](#)).

- 3 Click the Base Unit Info tab.

The Base Unit Info tab opens ([Figure 24](#)).

In a stack environment, if the base unit number does not begin with the number one, the information will not be displayed. Use the console interface and the Web-based management interface to change your base unit number. For detailed information, refer to *Using the Baystack 425 10/100/1000 Switch* and *Using Web-Based Management for the BayStack 425 10/100/1000 Switch*.

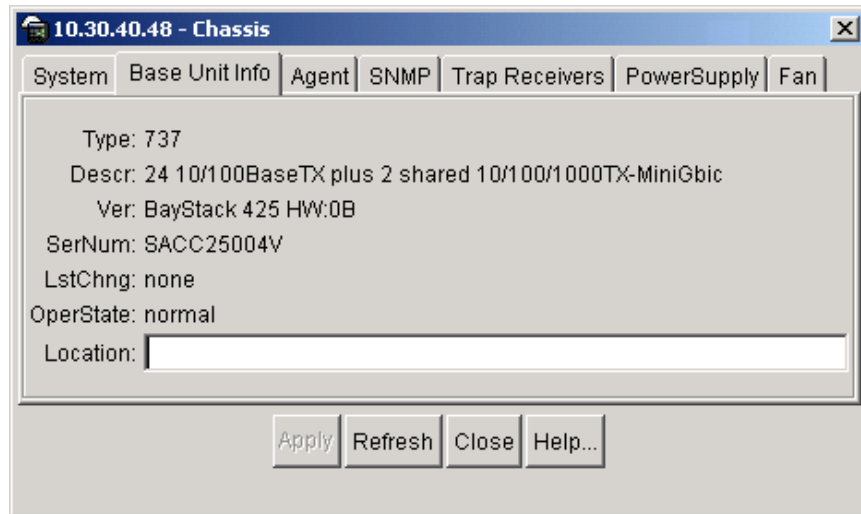
**Figure 24** Edit Chassis dialog box — Base Unit Info tab

Table 17 describes the Base Unit Info tab items.

**Table 17** Base Unit Info tab items

Item	Description
Type	The switch type.
Descr	A description of the switch hardware, including number of ports and transmission speed.
Ver	The switch hardware version number.
SerNum	The switch serial number.
LstChng	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
Location	Type the physical location of the switch.

## Stack Info tab

Like the Base Unit Info tab, the Stack Info tab provides read-only information about the operating status of the *stacked* switches and whether or not the default factory settings are being used. This tab is enabled for a stack of Baystack 420/425es.

To open the Stack Info tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens with the System tab displayed ([Figure 23](#)).

- 3 Click the Stack Info tab.

The Stack Info tab opens ([Figure 25](#)).

**Figure 25** Edit Chassis dialog box — Stack Info tab

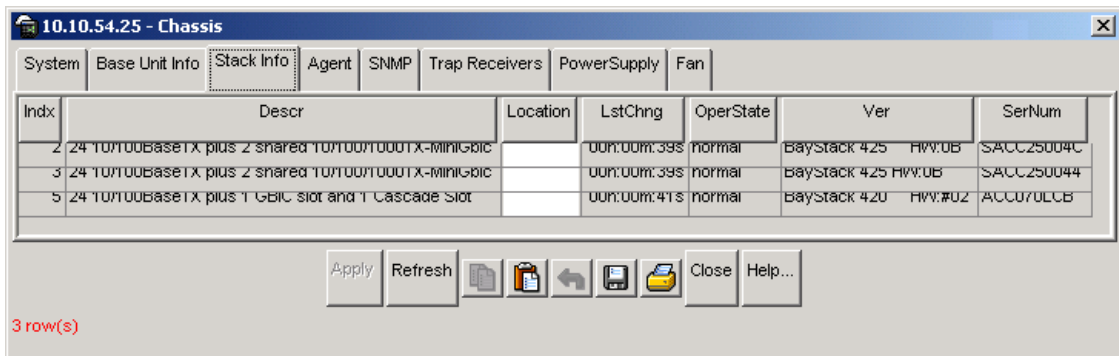


Table 18 describes the Stack Info tab fields.

**Table 18** Stack Info tab fields

Field	Description
Descr	A description of the component or subcomponent. If not available, the value is a zero length string.
Location	<p>The geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected together to exchange management information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: '4th flr wiring closet in blg A'.</p> <p>Notes: 1. This object is applicable only to components that can be found in either the Board or Unit groups. If the information is unavailable, for example, the chassis is not modeling a virtual chassis or component is not in Board or Unit group, the value is a zero length string.</p> <p>2. If this object is applicable and is not assigned a value through a SNMP SET PDU when the row is created, the value will default to the value of the object s5ChasComSerNum.</p>
LstChng	The value of sysUpTime when it was detected that the component/sub-component was added to the chassis. If this has not occurred since the cold/warm start of the agent, then the value is zero.
AdminState	<p>The state of the component or subcomponent. The values that are read-only are:</p> <ul style="list-style-type: none"> <li>• other — currently in some other state</li> <li>• notAvail — actual value is not available</li> </ul> <p>The possible values that can be read and written are:</p> <ol style="list-style-type: none"> <li>1. disable—disables operation</li> <li>2. enable—enables operation</li> <li>3. reset—resets component</li> <li>4. test—starts self test of component, with the result to be normal, warning, nonFatalErr, or fatalErr in object s5ChasComOperState</li> </ol> <p>The allowable (and meaningful) values are determined by the component type.</p>

**Table 18** Stack Info tab fields (continued)

Field	Description
OperState	The current operational state of the component. The possible values are: <ul style="list-style-type: none"><li>• other—some other state</li><li>• notAvail—state not available</li><li>• removed—component removed</li><li>• disabled—operation disabled</li><li>• normal—normal operation</li><li>• resetInProg—reset in progress</li><li>• testing—doing a self test</li><li>• warning—operating at warning level</li><li>• nonFatalErr—operating at error level</li><li>• fatalErr—error stopped operation</li></ul> The allowable (and meaningful) values are determined by the component type.
Ver	The version number of the component or subcomponent. If not available, the value is a zero length string.
SerNum	The serial number of the component or subcomponent. If not available, the value is a zero length string.

## Agent tab

The Agent tab provides read-only information about the addresses that the agent software uses to identify the switch.

To open the Agent tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens ([Figure 23 on page 56](#)) with the System tab displayed.

- 3 Click the Agent tab.

The Agent tab opens ([Figure 26](#)).

**Figure 26** Edit Chassis dialog box — Agent tab

NextBootpAddr	NextBootNetMask	LoadServerAddr	ImageFileName	ValidFlag	BootRouterAddr	MacAddr
10.30.40.41	255.255.255.0	134.177.152.102	bs42x_30022.img	valid	0.0.0.0	00:09:97:a2:9c:40

1 row(s)

Table 19 describes the Agent tab fields.

**Table 19** Agent tab fields

Item	Description
NextBootpAddr	The IP address of the BootP server to be used the next time the switch is booted.
NextBootNetMask	The subnet mask to be used the next time the switch is booted.
LoadServerAddr	The IP address of the load server for the configuration file and/or the image file. If not used, then the value is 0.0.0.0.
ImageFileName	Name of the image file(s) currently associated with the interface. When the object is not used, the value is a zero length string.
ValidFlag	Indicates if the configuration and/or image file(s) were downloaded from this interface and if the file names have not been changed.
BootRouterAddr	The IP address of the boot router for the configuration file and/or the image file.
MacAddr	The switch's MAC address.

## SNMP tab

The SNMP tab provides read-only information about the addresses that the agent software uses to identify the switch.

To open the SNMP tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens ([Figure 23 on page 56](#)) with the System tab displayed.

- 3 Click the SNMP tab.

The SNMP tab opens ([Figure 27](#)).

**Figure 27** Edit Chassis dialog box — SNMP tab

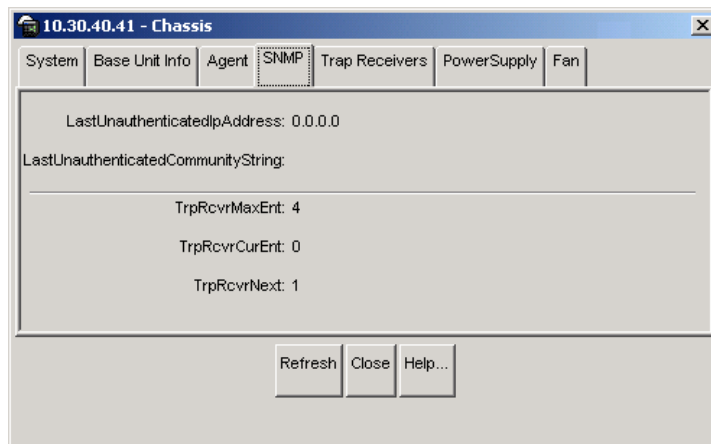




Table 20 describes the SNMP Info tab fields.

**Table 20** SNMP tab fields

Field	Description
LastUnauthenticatedIpAddress	The last IP address that was not authenticated by the device.
LastUnauthenticatedCommunityString	The last community string that was not authenticated by the device.
TrpRcvrMaxEnt	The maximum number of trap receiver entries.
TrpRcvrCurEnt	The current number of trap receiver entries.
TrpRcvrNext	The next trap receiver entry to be created.

## Trap Receivers tab

The Trap Receivers tab lists the devices that will receive SNMP traps from the BayStack 420/425 switch.

To open the Trap Receivers tab:

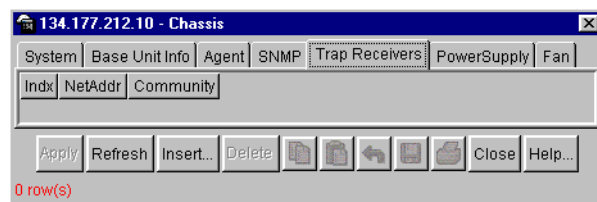
- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens (Figure 23 on page 56) with the System tab displayed.

- 3 Click the Trap Receivers tab.

The Trap Receivers tab opens (Figure 28).

**Figure 28** Trap Receivers tab



[Table 21](#) describes the Trap Receivers tab items.

**Table 21** Edit Chassis dialog box — Trap Receivers tab items

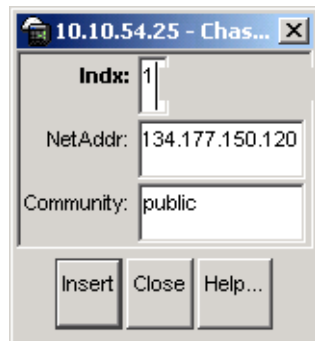
Item	Description
NetAddr	The address (or DNS hostname) for the trap receiver.
Community	Community string used for trap messages to this trap receiver.

## Adding a Trap Receiver

To edit the network traps table:

- 1 In the Trap Receivers tab ([Figure 28](#)), click Insert.  
The Chassis, Insert Trap Receive dialog box opens ([Figure 29](#)).

**Figure 29** Chassis, Insert Trap Receive dialog box



- 2 Type the Index, NetAddr, and the Community information.



**Note:** Refer to [Table 21 on page 66](#) for description of the Chassis, Insert Trap Receivers dialog box items.

---

- 3 Click Insert.

## Power Supply tab

The Power Supply tab provides read-only information about the operating status of the switch power supplies.

To open the PowerSupply tab:

- 1** Select the chassis.
- 2** From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens ([Figure 23](#)) with the System tab displayed.

- 3** Click the PowerSupply tab.

The PowerSupply tab opens ([Figure 30](#)).

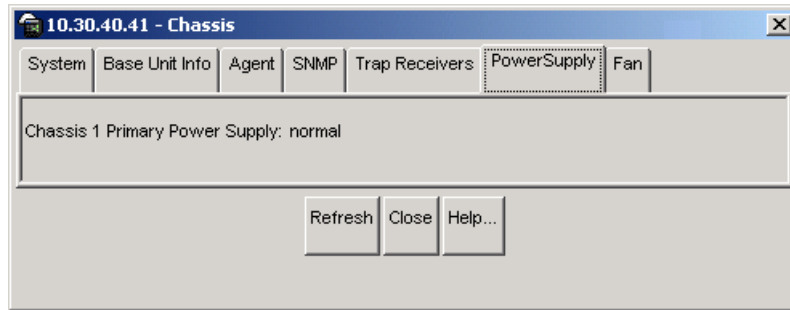
**Figure 30** Edit Chassis dialog box — Power Supply tab

Table 22 describes the Power Supply tab fields.

**Table 22** Power Supply tab fields

Field	Description
Desc	The power supply type.
OperStat	The operational state of the power supply. Possible values include: <ul style="list-style-type: none"><li>• other: Some other state.</li><li>• notAvail: State not available.</li><li>• removed: Component was removed.</li><li>• disabled: Operation disabled.</li><li>• normal: State is in normal operation.</li><li>• resetInProg: There is a reset in progress.</li><li>• testing: System is doing a self test.</li><li>• warning: System is operating at a warning level.</li><li>• nonFatalErr: System is operating at error level.</li><li>• fatalErr: A fatal error stopped operation.</li><li>• notConfig: A module needs to be configured. The allowable values are determined by the component type.</li></ul>

## Fan tab

The Fan tab provides read-only information about the operating status of the switch fans.

To open the Fan tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens ([Figure 23 on page 56](#)) with the System tab displayed.

- 3 Click the Fan tab.

The Fan tab opens ([Figure 31](#)).

**Figure 31** Edit Chassis dialog box — Fan tab

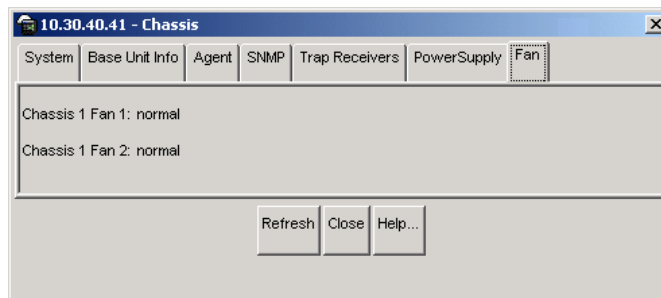


Table 23 describes the Fan tab fields.

**Table 23** Fan tab fields

Field	Description
Desc	The fan type.
OperStat	The operational state of the fan. Values include: <ul style="list-style-type: none"><li>• other: Some other state.</li><li>• notAvail: This state is not available.</li><li>• removed: Fan was removed.</li><li>• disabled: Fan is disabled.</li><li>• normal: Fan is operating in normal operation.</li><li>• resetInProg: A reset of the fan is in progress.</li><li>• testing: Fan is doing a self test.</li><li>• warning: Fan is operating at a warning level.</li><li>• nonFatalErr: Fan is operating at error level.</li><li>• fatalErr: An error stopped the fan operation</li><li>• notConfig: Fan needs to be configured. The allowable values are determined by the component type.</li></ul>

## Working with configuration files

You can view information and upload or download the configuration and image files from the Edit FileSystem dialog box.

To open the Edit FileSystem dialog box:

- ➡ From the Device Manager main menu, choose Edit > File System.

The FileSystem dialog box opens (Figure 32) and displays the Config/Image/Diag tab.

**Figure 32** FileSystem - Config/Image/Diag File tab dialog box

10.30.40.41 - FileSystem

Config/Image/Diag file    Ascii Config File

LoadServerAddr: 47.80.33.101

BinaryConfigFileName: config.cfg

ImgFileName: bs42x\_30036.img

FwFileName(Diag):

Action: ☒ other   ☐ dnldConfig   ☐ dnldImg   ☐ upldConfig   ☐ dnldFw

Status: other

Apply   Refresh   Close   Help...

Table 24 describes the FileSystem Config/Image/Diag file dialog box items.

**Table 24** FileSystem Config/Image/Diag file dialog box items

Item	Description
LoadServerAddr	The IP address of the load server for the configuration file and/or the image file. If not used, then the value is 0.0.0.0.
ConfigFileName	Name of the configuration file currently associated with the interface. When not used, the value is a zero length string.
ImageFileName	Name of the image file(s) currently associated with the interface. When the object is not used, the value is a zero length string.
FwFileName (Diag)	Specifies the FWFileName.

**Table 24** FileSystem Config/Image/Diag file dialog box items (continued)

Item	Description
Action	<ul style="list-style-type: none"><li>• This object is used to download or upload a config file or an image file. In read operation, if there is no action taken since the boot up, it will return with a value of other. Otherwise, it will return the latest action such as: dnldConfig dnldImg upldConfig</li><li>• In a write operation, the value that can be written is: dnldConfig - download a config file to a device.</li><li>• The new config file will not take effect until the next boot cycle of the device. Possible values are: dnldImg - download an image to a device. upldConfig - upload a config file to a server from a device.</li></ul>
Result	<p>This object is used to get the status of the latest action as shown by s5AgInfoFileAction. The values that can be read are:</p> <ul style="list-style-type: none"><li>• other — if no action taken since the boot up</li><li>• inProgress — the operation is in progress</li><li>• success — the operation succeeds.</li><li>• fail — the operation failed.</li></ul>

## ASCII config file

To see the ASCII Config file dialog box:

- ➡ In the Config/Image/Diag File tab, click on the ASCII Config tab..

The FileSystem - ASCII Config File dialog box ([Figure 33](#)) opens.



**Figure 33** File system - ASCII Config File dialog box

The screenshot shows a window titled "10.30.40.41 - FileSystem" with a tab labeled "Ascii Config File". Inside the window, there are two tabs: "Config/Image/Diag file" and "Ascii Config File". The "Ascii Config File" tab is active. It contains the following fields and controls:

- LoadServerAddr:** A text box containing "47.80.33.101".
- AsciiConfigFilename:** A text box containing "ascii.cfg".
- AsciiConfigAutoDownload:** A group of three radio buttons: "disabled" (selected), "useBootp", and "useConfig".
- AsciiConfigAutoDldStatus:** A label showing "passed".
- AsciiConfigManualDownload:** A group of two radio buttons: "downloadNow" (selected) and an unlabeled one.
- AsciiConfigManualDldStatus:** A label showing "passed".
- Buttons:** "Apply", "Refresh", "Close", and "Help..." at the bottom.

Table 25 describes the FileSystem - ASCII Config File dialog box items.

**Table 25** FileSystem - ASCII Config File dialog box items

Item	Description
LoadServerAddr	The IP address of the load server for the ASCII configuration file. If not used, then the value is 0.0.0.0.
ASCIIConfigFile Name	Name of the ASCII configuration file currently associated with the interface. When not used, the value is a zero length string.
ASCIIConfigAuto Download	Specifies automatic ASCII configuration download.
ASCIIConfigAuto dldStatus	Specifies the current status of the ASCII configuration file download.
ASCIIConfigMan ualDownload	Specifies manual download of an ASCII configuration file.
ASCIIConfigMan ualDldStatus	Specifies the current status of the manual download of an ASCII configuration file.

## Graphing chassis statistics

To graph chassis statistics:

- 1 Select the chassis.
- 2 Do *one* of the following:
  - From the shortcut menu, choose Graph.
  - From Device Manager main menu, choose Graph > Chassis.
  - On the toolbar, click Graph.



The following sections describe the Graph Chassis dialog box tabs with descriptions of the statistics on each tab.

Six columns provide the statistics for the counters that are listed on the tab.

For descriptions of the chassis IP statistics, refer to [Table 10 on page 39](#).

### SNMP tab

The chassis SNMP tab lists chassis statistics.

To open the SNMP tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Graph > Chassis.

The Chassis dialog box opens ([Figure 23 on page 56](#)) with the System tab displayed.

- 3 Click the SNMP tab.

The SNMP tab opens ([Figure 34](#)).

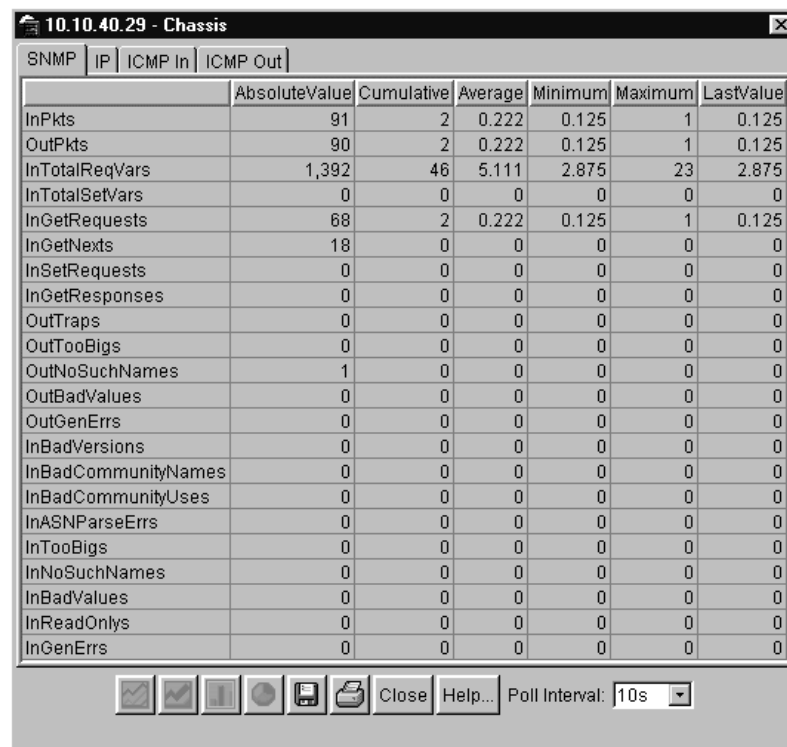
**Figure 34** Graph Chassis dialog box — Chassis SNMP tab

Table 26 describes the SNMP tab fields.

**Table 26** SNMP tab fields

Field	Description
InPkts	The total number of messages delivered to the SNMP from the transport service.
OutPkts	The total number of SNMP messages passed from the SNMP protocol to the transport service.
InTotalReqVars	The total number of MIB objects retrieved successfully by the SNMP protocol as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
InTotalSetVars	The total number of MIB objects altered successfully by the SNMP protocol as the result of receiving valid SNMP Set-Request PDUs.

**Table 26** SNMP tab fields (continued)

Field	Description
InGetRequests	The total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol.
InGetNexts	The total number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol.
InSetRequests	The total number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol.
InGetResponses	The total number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol.
OutTraps	The total number of SNMP Trap PDUs generated by the SNMP protocol.
OutTooBigs	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is tooBig.
OutNoSuchNames	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is noSuchName.
OutBadValues	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is badValue.
OutGenErrs	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is genErr.
InBadVersions	The total number of SNMP messages delivered to the SNMP protocol for an unsupported SNMP version.
InBadCommunityNames	The total number of SNMP messages delivered to the SNMP protocol that used an unknown SNMP community name.
InBadCommunityUses	The total number of SNMP messages delivered to the SNMP protocol that represented an SNMP operation not allowed by the SNMP community named in the message.
InASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP protocol when decoding received SNMP messages.
InTooBigs	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is tooBig.
InNoSuchNames	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is noSuchName.
InBadValues	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is badValue.

**Table 26** SNMP tab fields (continued)

Field	Description
InReadOnlys	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is readOnly. It is a protocol error to generate an SNMP PDU containing the value “readOnly” in the error-status field. This object is provided to detect incorrect implementations of the SNMP.
InGenErrs	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is genErr.

## IP tab

The IP tab shows IP information for the chassis.

To open the IP tab:

- 1 Select the chassis.
- 2 Do *one* of the following:
  - From Device Manager main menu, choose Graph > Chassis.
  - From the shortcut menu, choose Graph.
  - On the toolbar, click Graph.

The Chassis dialog box opens ([Figure 34 on page 75](#)) with the SNMP tab displayed.

- 3 Click the IP tab.

The IP tab opens ([Figure 35](#)).

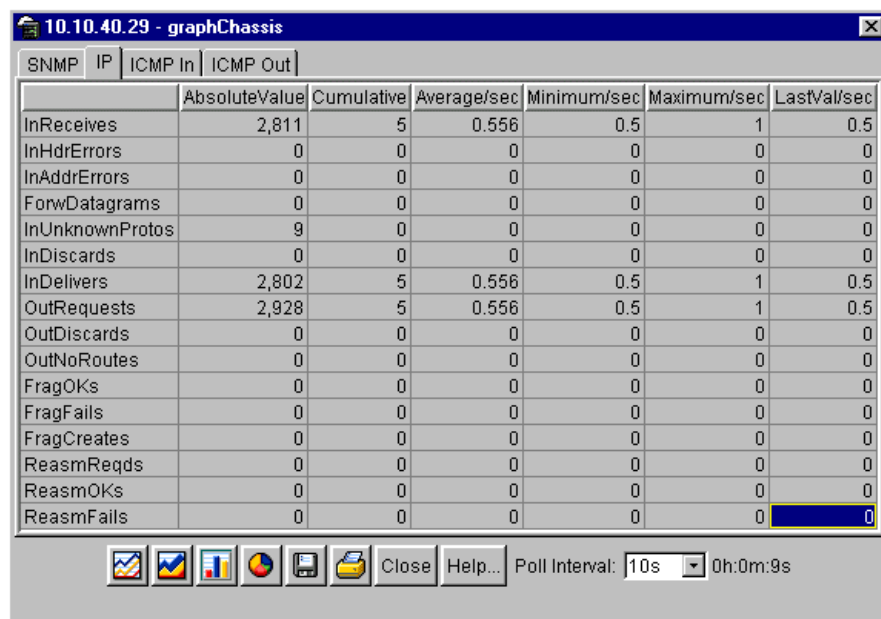
**Figure 35** Graph Chassis dialog box — IP tab

Table 27 describes the Chassis IP tab fields

**Table 27** Chassis IP tab fields

Field	Description
InReceives	The total number of input datagrams received from interfaces, including those received in error.
InHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options.
InAddrErrors	The number of input datagrams discarded because the IP address in the IP header destination field was not a valid address. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For addresses that are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

**Table 27** Chassis IP tab fields (continued)

Field	Description
ForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. For addresses that do not act as IP Gateways, this counter will include only those packets that were Source-Routed by way of this address and had successful Source-Route option processing.
InUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing but that were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting reassembly.
InDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	The total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
OutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
OutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter also includes any packets counted in ipForwDatagrams that have no route. Note that this includes any datagrams a host cannot route because all of its default gateways are down.
FragOKs	The number of IP datagrams that have been successfully fragmented at this entity.
FragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, for example, because their Don't Fragment flag was set.
FragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
ReasmReqds	The number of IP fragments received that needed to be reassembled at this entity.

**Table 27** Chassis IP tab fields (continued)

Field	Description
ReasmOKs	The number of IP datagrams successfully reassembled.
ReasmFails	The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

## ICMP In tab

The chassis ICMP In tab shows ICMP In statistics.

To open the ICMP In tab:

- 1 Select the chassis.
- 2 Do *one* of the following:
  - From Device Manager main menu, choose Graph > Chassis.
  - From the shortcut menu, choose Graph.
  - On the toolbar, click Graph.

The Chassis dialog box opens ([Figure 34 on page 75](#)) with the SNMP tab displayed.

- 3 Click the ICMP In tab.

The ICMP In tab opens ([Figure 36](#)).



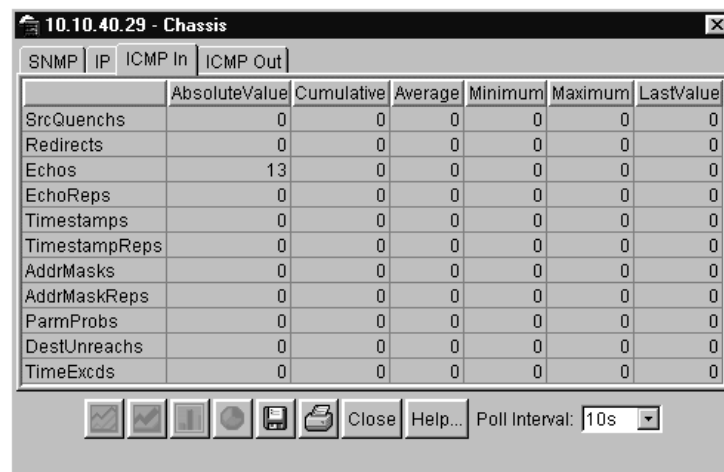
**Figure 36** Graph Chassis dialog box — ICMP In tab

Table 28 describes the ICMP In tab fields.

**Table 28** ICMP In tab fields

Field	Description
SrcQuenchs	The number of ICMP Source Quench messages received.
Redirects	The number of ICMP Redirect messages received.
Echos	The number of ICMP Echo (request) messages received.
EchoReps	The number of ICMP Echo Reply messages received.
Timestamps	The number of ICMP Timestamp (request) messages received.
TimestampReps	The number of ICMP Timestamp Reply messages received.
AddrMasks	The number of ICMP Address Mask Request messages received.
AddrMaskReps	The number of ICMP Address Mask Reply messages received.
ParmProbs	The number of ICMP Parameter Problem messages received.
DestUnreachs	The number of ICMP Destination Unreachable messages received.
TimeExcds	The number of ICMP Time Exceeded messages received.

## ICMP Out tab

The chassis ICMP Out shows ICMP Out statistics.

To open the ICMP Out tab:

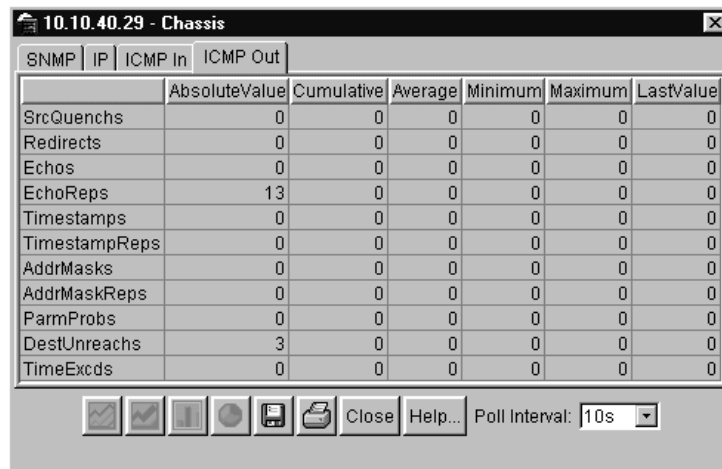
- 1 Select the chassis.
- 2 Do *one* of the following:
  - From Device Manager main menu, choose Graph > Chassis.
  - From the shortcut menu, choose Graph.
  - On the toolbar, click Graph.

The Chassis dialog box opens ([Figure 34 on page 75](#)) with the SNMP tab displayed.

- 3 Click the ICMP Out tab.

The ICMP Out tab opens ([Figure 37](#)).

**Figure 37** Graph Chassis dialog box — ICMP Out tab



[Table 29](#) describes the ICMP Out tab fields.

**Table 29** ICMP Out tab fields

Field	Description
SrcQuenchs	The number of ICMP Source Quench messages sent.
Redirects	The number of ICMP Redirect messages received. For a host, this object will always be zero, because hosts do not send redirects.
Echos	The number of ICMP Echo (request) messages sent.
EchoReps	The number of ICMP Echo Reply messages sent.
Timestamps	The number of ICMP Timestamp (request) messages sent.
TimestampReps	The number of ICMP Timestamp Reply messages sent.
AddrMasks	The number of ICMP Address Mask Request messages sent.
AddrMaskReps	The number of ICMP Address Mask Reply messages sent.
ParmProbs	The number of ICMP Parameter Problem messages sent.
DestUnreachs	The number of ICMP Destination Unreachable messages sent.
TimeExcds	The number of ICMP Time Exceeded messages sent.



---

## Chapter 3

# Configuring and graphing ports

---

This chapter describes how you use Device Manager to configure and graph ports on a Baystack 420/425 Switch.

The windows displayed when you configure a single port differ from the ones displayed when you configure multiple ports. However, the options are similar.

## Viewing and editing a single port configuration

To view or edit the configuration of a single or multiple ports:

- 1 Double-click on a single port or select the ports you want to edit.
- 2 Do one of the following:
  - From the shortcut menu, choose Edit.
  - From the Device Manager main menu, choose Edit > Port.
  - Double-click on the selected port.
  - On the toolbar, click Edit.



**Note:** When you edit a single port, tabs that are not applicable are not available for you to select.

When you edit multiple ports, some tabs are not available, and some tabs are available even though the options are not applicable. When the option does not apply for a given port, NoSuchObject is displayed.

---

The following sections provide a description of the tabs in the Edit Port dialog box, and details about each field on the tab.

## Interface tab for a single port

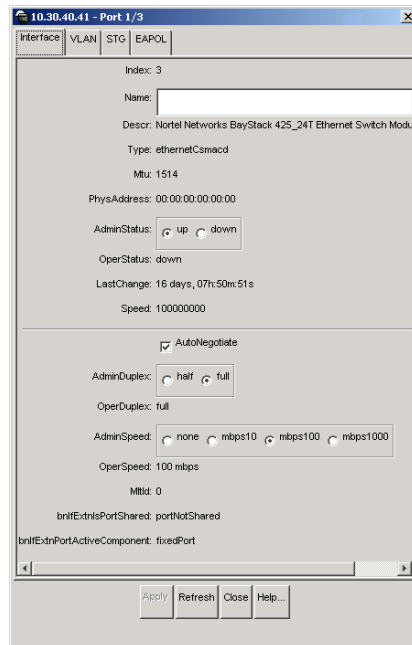
The Interface tab shows the basic configuration and status of a single port.

To view the Interface tab:

- 1 Select the port you want to edit.
- 2 Do one of the following:
  - Double-click on the selected port
  - From the shortcut menu, choose Edit.
  - From the Device Manager main menu, choose Edit > Port.
  - On the toolbar, click Edit button.

The Port dialog box for a single port opens (Figure 38) with the Interface tab displayed.

**Figure 38** Port dialog box — Interface tab





**Note:** 10/100BASE-TX ports may not autonegotiate correctly with older 10/100BASE-TX equipment. In some cases, the older devices can be upgraded with new firmware or driver revisions. If an upgrade does not allow autonegotiation to correctly identify the link speed and duplex settings, you can manually configure the settings for the link in question. Check the Nortel Networks Web site ([support.baynetworks.com/software](http://support.baynetworks.com/software)) for the latest compatibility information.

Table 30 describes the Interface tab items for a single port.

**Table 30** Interface tab items for a single port

Field	Description
Index	A unique value assigned to each interface. The value ranges between 12 and 255.
Name	Specifies a name for the port.
Descr	The type of switch and number of ports.
Type	The media type of this interface.
Mtu	The size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	The MAC address assigned to a particular interface.
AdminStatus	<p>The current administrative state of the interface, which can be one of the following:</p> <ul style="list-style-type: none"><li>• up</li><li>• down</li></ul> <p>When a managed system is initialized, all interfaces start with AdminStatus in the down state. AdminStatus changes to the up state (or remains in the down state) as a result of either management action or the configuration information available to the managed system.</p>

**Table 30** Interface tab items for a single port (continued)

Field	Description
OperStatus	<p>The current operational state of the interface, which can be one of the following:</p> <ul style="list-style-type: none"> <li>• up</li> <li>• down</li> <li>• testing</li> </ul> <p>If AdminStatus is up, then OperStatus should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down, then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.</p>
LastChange	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
Speed	Current speed.
AutoNegotiate	Indicates whether this port is enabled for autonegotiation or not.
AdminDuplex	The current administrative duplex mode of the port (half or full).
AdminSpeed	Set the port's speed.
OperSpeed	The current operating speed of the port.
MltId	The MultiLink Trunk to which the port is assigned (if any).
OperDuplex	The current mode of the port (half duplex or full duplex).
IsPortShared	Specifies whether a port is shared. Multiple ports that are logically represented as a single port are shared. Only one shared port may be active at a time.
PortActiveComponent	Specifies the physical port components that are active for a shared port.

## VLAN tab for a single port

The VLAN tab allows you to view the VLAN membership for a single port.

To view the VLAN tab:

- 1 Select the port you want to edit.
- 2 Do one of the following:



- Double-click the selected port
- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit.

The Port dialog box for a single port opens (Figure 38 on page 86) with the Interface tab displayed.

**3** Click the VLAN tab.

The VLAN tab opens (Figure 39).

**Figure 39** Edit Port dialog box — VLAN tab

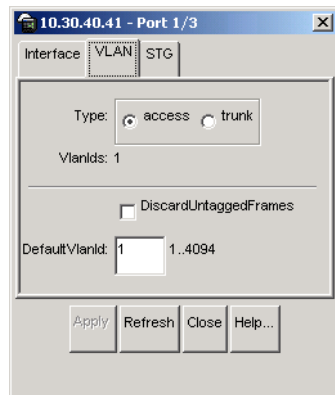


Table 31 describes the VLAN tab items.

**Table 31** VLAN tab items for a single port

Item	Description
Type	Indicates the type of VLAN port (Trunk or Access port). If the port is a trunk port, the port is probably a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN if there is no membership conflict.
Vlanids	The VLANIDs of which this port is a member.

**Table 31** VLAN tab items for a single port (continued)

Item	Description
DiscardUntaggedFrames	This field only applies to trunk ports. It acts as a flag used to determine how to process untagged frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are assigned to the VLAN specified by rcVlanPortDefaultVlanId.
DefaultVlanId	The VLAN ID assigned to untagged frames received on a trunk port.

# STG tab for a single port

In the Spanning Tree Group (STG) tab, you can view the status and modify the configuration of a port's spanning tree parameters.

To view the STG tab:

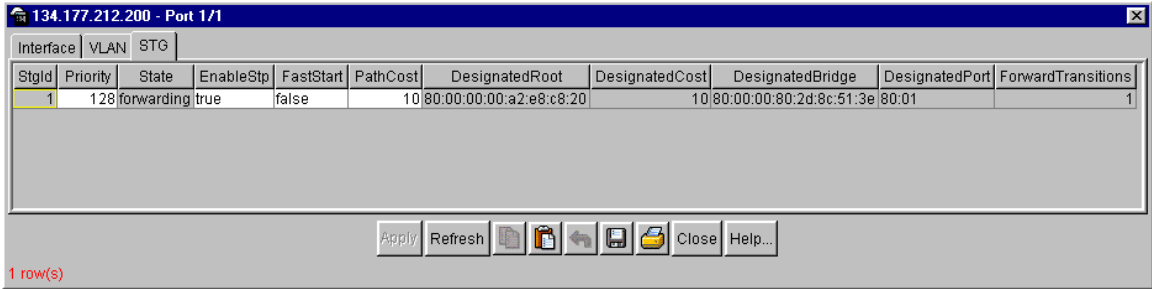
- 1 Select the port you want to edit.
- 2 Do one of the following:
  - Double-click the selected port.
  - From the shortcut menu, choose Edit.
  - From the Device Manager main menu, choose Edit > Port.
  - On the toolbar, click Edit.

The Port dialog box for a single port opens (Figure 38 on page 86) with the Interface tab displayed.

- 3 Click the STG tab.

The STG tab opens (Figure 40).

**Figure 40** Edit Port dialog box — STG tab



[Table 32](#) describes the STG tab items.

**Table 32** STG tab items for a single port

Item	Description
StgId	The number of times this port has transitioned from the Learning state to the Forwarding state.
Priority	The value of the priority field that is contained in the first (in network byte order) octet of the (2-octet long) Port ID. The other octet of the Port ID is derived from the value of dot1dStpPort.
State	The port's current state as defined by application of the Spanning Tree Protocol. This state controls the action a port takes when it receives a frame. If the bridge detects a port that is malfunctioning, it places that port into the broken state. For ports that are disabled (see EnableStp), this object has a value of disabled.
EnableStp	Allows you to select true or false to enable or disable STP.
FastStart	Allows you to select true or false to enable or disable FastStart.
PathCost	The contribution of this port to the cost of paths toward the spanning tree root, which include this port. The IEEE 802.1D-1990 standard recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN.
DesignatedRoot	The unique Bridge Identifier of the bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached.
DesignatedCost	The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.
DesignatedBridge	The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port's segment.
DesignatedPort	The Port Identifier of the port on the Designated Bridge for this port's segment.
ForwardTransitions	The number of times this port has transitioned from the Learning state to the Forwarding state.

## EAPOL tab for a single port

The EAPOL tab allows you to configure EAPOL-based security for a single port.

To view the EAPOL tab:

- 1** Select the port you want to edit.
- 2** Do one of the following:
  - Double-click the selected port
  - From the shortcut menu, choose Edit.
  - From the Device Manager main menu, choose Edit > Port.
  - On the toolbar, click Edit.

The Port dialog box for a single port opens [\(Figure 38\)](#) with the Interface tab displayed.

- 3** Click the EAPOL tab.

The EAPOL tab opens [\(Figure 41\)](#).

**Figure 41** Edit Port dialog box — EAPOL tab

10.20.30.100 - Port 1/3

Interface | VLAN | STG | **EAPOL**

- EAP security

PortProtocolVersion: 1

PortCapabilities: dot1xPaePortAuthCapable

☐ PortInitialize

☐ PortReauthenticate

- Authenticator configuration

PaeState: forceAuth

BackendAuthState: initialize

AdminControlledDirections: ☒ both ☐ in

OperControlledDirections: both

AuthControlledPortStatus: authorized

AuthControlledPortControl: ☐ forceUnauthorized ☐ auto ☒ forceAuthorized

QuietPeriod: 60

TxPeriod: 30

SuppTimeout: 30

ServerTimeout: 30

MaxReq: 2

Apply Refresh Close Help...

Table 33 describes the EAPOL tab items.

**Table 33** EAPOL tab items for a single port

Item	Description
PortProtocolVersion	The EAP Protocol version that is running on this port.
PortCapabilities	The PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable(0).
PortInitialize	Setting this attribute to True causes this port's EAPOL state to be initialized.
PortReauthenticate	Setting this attribute to True causes the reauthentication of the client.
PaeState	The current authenticator PAE state machine stat value.

**Table 33** EAPOL tab items for a single port (continued)

Item	Description
BackendAuthState	The current state of the Backend Authentication state machine.
AdminControlledDirections	The current value of the administrative controlled directions parameter for the port.
OperControlledDirections	The current value of the operational controlled directions parameter for the port.
AuthControlledPortStatus	The current value of the controlled port status parameter for the port.
AuthControlledPortControl	The current value of the controlled port control parameter for the port.
QuietPeriod	The current value of the time interval between authentication failure and the start of a new authentication.
TxPeriod	Time to wait for response from supplicant for EAP requests/ Identity packets.
SuppTimeout	Time to wait for response from supplicant for all EAP packets except EAP Request/Identity.
ServerTimeout	Time to wait for a response from the RADIUS server
MaxReq	Number of times to retry sending packets to the supplicant.
ReAuthPeriod	Time interval between successive re-authentications.
ReAuthEnabled	Whether to re-authenticate or not. Setting this object to Enabled causes reauthentication of existing supplicant at the time interval specified in the Re-authentication Period field.
KeyTxEnabled	The value of the KeyTransmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns false as key transmission is irrelevant.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

## Viewing and editing multiple port configurations

To view or edit the configurations of multiple ports:

- 1 Select the ports you want to edit.

Press [Ctrl] + left click the ports you want to view or configure. A yellow outline appears around the selected ports.

**2** Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- Double-click on the selected port.
- On the toolbar, click Edit.



---

**Note:** When you edit multiple ports, some tabs are not available, and some tabs are available even though the options are not applicable. When the option does not apply for a given port, NoSuchObject is displayed.

---



## Graphing multiple ports

You can graph port statistics from the graph port dialog box.

To open the graph port dialog box:

- 1 Select the port or ports you want to graph.
- 2 Do one of the following:
  - From the shortcut menu, choose Graph.
  - From the Device Manager main menu, choose Graph > Port.
  - On the toolbar, click Graph.



The following sections discuss the graph port statistics tabs with descriptions of the statistics.



**Note:** Some statistics are only available when you graph a single port.

---

### Interface tab for multiple ports

The Interface tab shows the basic configuration and status of the selected ports.

To view or edit the Interface tab for multiple ports:

- 1 Select the ports that you want to edit.  
[Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

**2** Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit.

The Interface tab ([Figure 42](#)) shows port interface statistics.

**Figure 42** Graph Port dialog box — Interface tab

Index	Port	Name	Descr	Type	Mtu	PhysAddress	AdminStatus	OperStatus	LastChange	Speed	AutoNegotiate	AdminDuplex	OperDuplex	AdminSpeed	OperSpeed	Mbit/s	Error
3	1/3		None...	etne...	15...	00:00:00:00:...	up	down	35 days, 1...	1000...	true	full	full	1000...	1000	0	portin
5	1/5		None...	etne...	15...	00:00:00:00:...	up	down	35 days, 1...	1000...	true	full	full	1000...	1000	0	portin
7	1/7		None...	etne...	15...	00:00:00:00:...	up	down	35 days, 1...	1000...	true	full	full	1000...	1000	0	portin

3 row(s)

[Table 34](#) describes the Interface tab fields.

**Table 34** Interface tab fields for multiple ports

Field	Description
Index	A unique value assigned to each interface. The value ranges between 1 and 255.
Descr	Type of switch and number of ports.
Type	Media type for this interface.
Mtu	Size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	MAC address assigned to a particular interface.
AdminStatus	<p>Current administrative state of the interface, which can be one of the following:</p> <ul style="list-style-type: none"> <li>• up</li> <li>• down</li> </ul> <p>When a managed system is initialized, all interfaces start with AdminStatus in the down state. AdminStatus changes to the up state (or remains in the down state) as a result of either management action or the configuration information available to the managed system.</p>

**Table 34** Interface tab fields for multiple ports (continued)

Field	Description
OperStatus	<p>Current operational state of the interface, which can be one of the following:</p> <ul style="list-style-type: none"> <li>• up</li> <li>• down</li> <li>• testing</li> </ul> <p>If AdminStatus is up, then OperStatus should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down, then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.</p>
LastChange	Value of the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
Speed	The estimate bandwidth of the interface in bits per second (bps). For interfaces that do not vary in bandwidth or have no way to estimate the bandwidth, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reported by the object, then the object displays its maximum value (4,294,967,295). For a sub-layer that has no concept of bandwidth, the object should be zero.
AutoNegotiate	Indicates whether the port is enabled (checked) for autonegotiation or not.
AdminDuplex	The current administrative duplex mode of the port (half or full).
OperDuplex	Indicate current duplex value of the port.
AdminSpeed	Set the speed of a port: none, mbps10, and mbps100
OperSpeed	The current operating speed of the port.
MltId	The MultiLink Trunk to which the port is assigned (if any).
IsPortShared	Specifies whether a port is shared. Multiple ports that are logically represented as a single port are shared. Only one shared port may be active at a time.
PortActiveComponent	Specifies the physical port components that are active for a shared port.

## VLAN tab for multiple ports

The VLAN tab shows the VLAN membership for the selected ports.

To view or edit the Interface tab for multiple ports:

- 1 Select the ports that you want to edit.

[Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

- 2 Do one of the following:

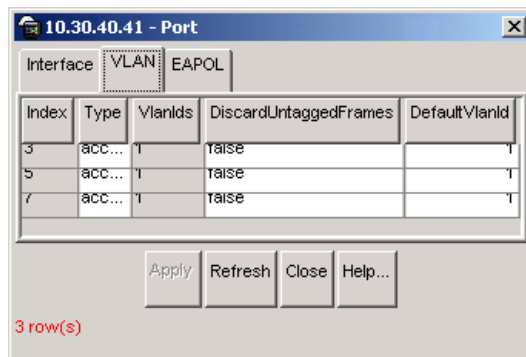
- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit.

The Port dialog box for a multiple port ([Figure 38 on page 86](#)) opens with the Interface tab displayed.

- 3 Click the VLAN tab.

The VLAN tab opens ([Figure 43](#)).

**Figure 43** VLAN tab for multiple ports



[Table 35](#) describes the VLAN tab fields for multiple ports.

**Table 35** VLAN tab fields for multiple ports

Field	Description
Type	Indicates the type of VLAN port (Trunk or Access port). If the port is a trunk port, the port is probably a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN if there is no membership conflict.
VlanIds	The VLANIDs of which this port is a member.

**Table 35** VLAN tab fields for multiple ports (continued)

Field	Description
DiscardUntaggedFrames	This field only applies to trunk ports. It acts as a flag used to determine how to process untagged frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are assigned to the VLAN specified by rcVlanPortDefaultVlanId.
DefaultVlanId	The VLAN ID assigned to untagged frames received on a trunk port.

## EAPOL tab for multiple ports

The EAPOL tab shows EAPOL statistics for the selected ports.

To view or edit the EAPOL tab for multiple ports:

- 1 Select the ports that you want to edit.

[Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

- 2 Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit.

The Port dialog box for a multiple port ([Figure 38](#)) opens with the Interface tab displayed.

- 3 Click the EAPOL tab.

The EAPOL tab opens ([Figure 44](#)).

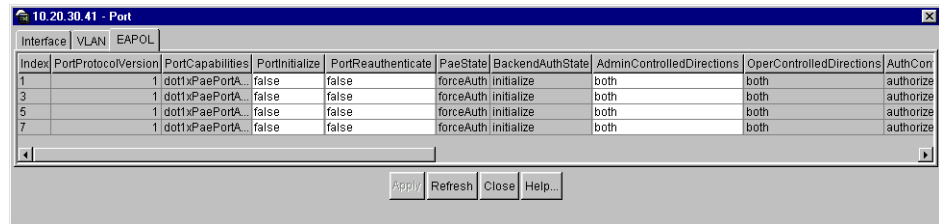
**Figure 44** EAPOL tab for multiple ports

Table 36 describes the EAPOL tab fields for multiple ports.

**Table 36** EAPOL tab fields for multiple ports

Field	Description
Index	Displays the unique value assigned to each interface.
PortProtocolVersion	The EAP Protocol version that is running on this port.
PortCapabilities	The PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable(0).
PortInitialize	Setting this attribute to True causes this port's EAPOL state to be initialized.
PortReauthenticate	Setting this attribute to True causes the reauthentication of the client.
PaeState	The current authenticator PAE state machine stat value.
BackendAuthState	The current state of the Backend Authentication state machine.
AdminControlledDirections	The current value of the administrative controlled directions parameter for the port.
OperControlledDirections	The current value of the operational controlled directions parameter for the port.
AuthControlledPortStatus	The current value of the controlled port status parameter for the port.
AuthControlledPortControl	The current value of the controlled port control parameter for the port.
QuietPeriod	The current value of the time interval between authentication failure and the start of a new authentication.
TxPeriod	Time to wait for response from supplicant for EAP requests/identity packets.

**Table 36** EAPOL tab fields for multiple ports (continued)

Field	Description
SuppTiemout	Time to wait for response from supplicant for all EAP packets except EAP Request/Identity.
ServerTimeout	Time to wait for a response from the RADIUS server
MaxReq	Number of times to retry sending packets to the supplicant.
ReAuthPeriod	Time interval between successive re-authentications.
ReAuthEnabled	Whether to re-authenticate or not. Setting this object to Enabled causes reauthentication of existing supplicant at the time interval specified in the Re-authentication Period field.
KeyTxEnabled	The value of the KeyTranmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns false as key transmission is irrelevant.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

## Graphing port statistics

You can graph statistics for either a single port or multiple ports from the graphPort dialog box. The windows displayed are identical for either single or multiple port configuration.

To open the graphPort dialog box for graphing:

- 1 Select the port or ports you want to graph.  
To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.
- 2 Do one of the following:
  - From the Device Manager main menu, choose Graph > Port.
  - From the shortcut menu, choose Graph.
  - On the toolbar, click Graph.

The graphPort dialog box for a single port ([Figure 45 on page 104](#)) or for multiple ports opens with the Interface tab displayed.

## Interface tab for graphing ports

The Interface tab shows interface parameters for graphing a port or ports.

To open the Interface tab for graphing:

- 1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

- 2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port ([Figure 45 on page 104](#)) or for multiple ports opens with the Interface tab displayed.

**Figure 45** Interface tab for graphing ports

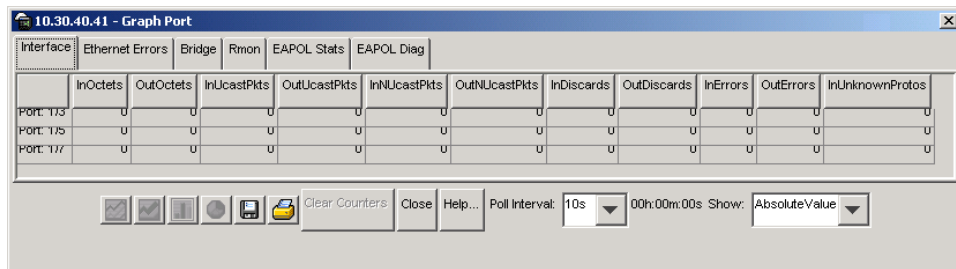




Table 37 describes the Interface tab fields for graphing ports.

**Table 37** Port Interface tab fields for multiple ports

Field	Description
ifInOctets	The total number of octets received on the interface, including framing characters.
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters.
ifInUcastPkts	The number of packets delivered by this sublayer to a higher sublayer that were not addressed to a multicast or broadcast address at this sublayer.
ifOutUcastPkts	The number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast address at this sublayer. This total number includes those packets discarded or unsent.
ifInNUcastPkts	The number of packets delivered by this sublayer to a higher (sub)layer, which were addressed to a multicast or broadcast address at this sublayer.
ifOutNUcastPkts	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent.
InDiscards	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
OutDiscards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
InErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.

**Table 37** Port Interface tab fields for multiple ports (continued)

Field	Description
OutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
InUnknownProtos	For packet-oriented interfaces, the number of packets received via the interface that were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received via the interface that were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0.

## Ethernet Errors tab for graphing ports

The port Ethernet Errors tab shows port Ethernet Errors statistics.

To open the Ethernet Errors tab for graphing:

- 1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

**2** Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port ([Figure 38 on page 86](#)) or for multiple ports opens with the Interface tab displayed.

**3** Click the Ethernet Errors tab.

The Ethernet Errors tab opens ([Figure 46](#)).

**Figure 46** Graph Port dialog box — Ethernet Errors tab

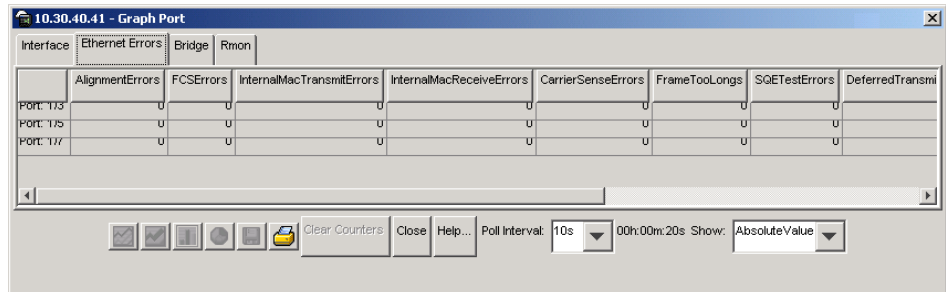


Table 44 describes the Ethernet Errors tab fields.

**Table 38** Ethernet Errors tab fields

Field	Description
AlignmentErrors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
InternalMacTransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.
InternalMacReceiveErrors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object.  The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.
CarrierSenseErrors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.

**Table 38** Ethernet Errors tab fields (continued)

Field	Description
FrameTooLongs	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
SQETestErrors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
DeferredTransmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveCollisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.

## Bridge tab

The Bridge tab displays port frame statistics.

To open the Bridge tab for graphing:

- 1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

- 2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port ([Figure 38 on page 86](#)) or for multiple ports opens with the Interface tab displayed.

- 3 Click the Bridge tab.

The Bridge tab for graphing ports opens ([Figure 47](#)).

**Figure 47** Graph Port dialog box — Bridge tab

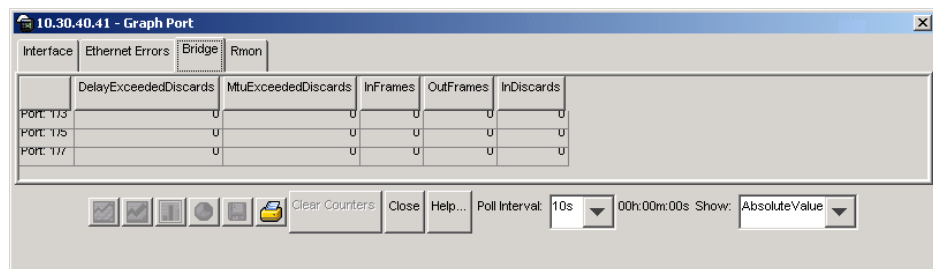


Table 39 describes the Bridge tab fields.

**Table 39** Bridge tab fields

Field	Description
DelayExceededDiscards	Number of frames discarded by the port due to excessive transit delays through the bridge. It is incremented by both transparent and source route bridges.
MtuExceededDiscards	Number of frames discarded by the port due to an excessive size. It is incremented by both transparent and source route bridges.
InFrames	The number of frames that have been received by this port from its segment.
OutFrames	The number of frames that have been received by this port from its segment.
InDiscards	Count of valid frames received which were discarded (filtered) by the Forwarding Process.

## RMON tab

The RMON tab displays Ethernet statistics for graphing a port or ports.

To open the RMON tab for graphing:

- 1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

**2** Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port (Figure 38 on page 86) or for multiple ports opens with the Interface tab displayed.

**3** Click the RMON tab.

The RMON tab for graphing ports opens (Figure 48).

**Figure 48** Graph Port dialog box — RMON tab

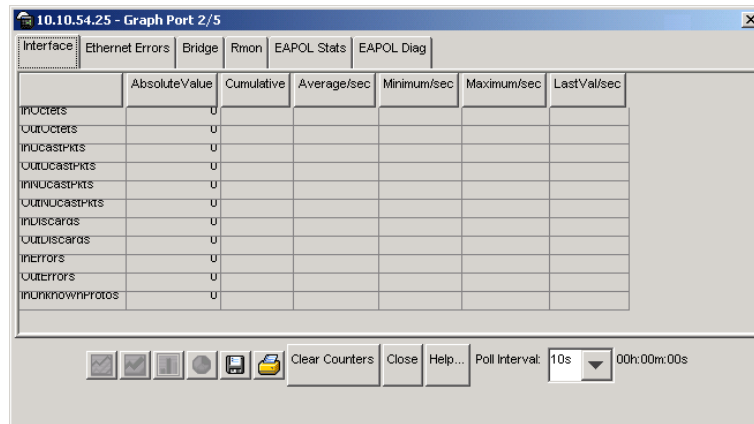


Table 40 describes the RMON tab fields.

**Table 40** RMON tab fields

Field	Description
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.



**Table 40** RMON tab fields (continued)

Field	Description
MulticastPkts	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
CRCAAlignErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
UndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
OversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
Fragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). It is entirely normal for etherStatsFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Jabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
<=64	The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets).
65 - 127	The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets).
128 - 255	The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets).
256 - 511	The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets).

**Table 40** RMON tab fields (continued)

Field	Description
512 - 1023	The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets).
>1023	The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets).

## EAPOL Stats tab for graphing ports

The EAPOL Stats tab displays EAPOL statistics.

To open the EAPOL Stats tab for graphing:

- 1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

- 2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed.

- 3 Click the EAPOL Stats tab.

The EAPOL Stats tab for graphing multiple ports opens ([Figure 49](#)).

**Figure 49** Graph Port dialog box — EAPOL Stats tab

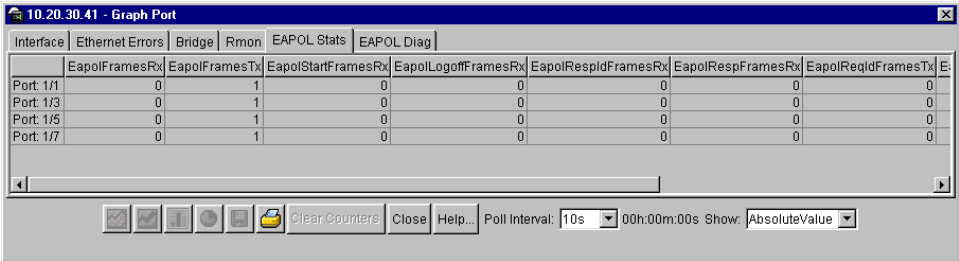


Table 41 describes the EAPOL tab fields.

**Table 41** EAPOL tab fields

Field	Description
EapolFramesRx	The number of valid EAPOL frames of any type that have been received by this authenticator.
EapolFramesTx	The number of EAPOL frame types of any type that have been transmitted by this authenticator.
EapolStartFramesRx	The number of EAPOL start frames that have been received by this authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this authenticator.
EapolRespIdFramesRx	The number of EAPOL Resp/Id frames that have been received by this authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (Other than Resp/Id frames) that have been received by this authenticator.
EapolReqIdFramesTx	The number of EAPOL Req/Id frames that have been transmitted by this authenticator.
EapolReqFramesTx	The number of EAP Req/Id frames (Other than Rq/Id frames) that have been transmitted by this authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this authenticator in which the packet body length field is not valid.

## EAPOL Diag tab for graphing ports

The EAPOL Diag tab displays EAPOL diagnostics statistics.

To open the EAPOL Diag tab for graphing:

- 1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

- 2 Do one of the following:

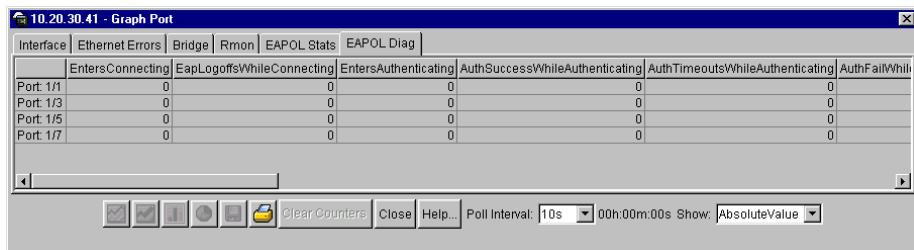
- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed.

- 3 Click the EAPOL Diag tab.

The EAPOL Diag tab for graphing multiple ports opens ([Figure 50](#)).

**Figure 50** Graph Port dialog box — EAPOL Diag tab



---

## Chapter 4

# Setting up MultiLink Trunk ports

---

MultiLink Trunking (MLT) is a point-to-point connection that aggregates multiple ports so that they logically act like a single port with the aggregated bandwidth. Grouping multiple ports into a logical link allows you to achieve higher aggregate throughput on a switch-to-switch or switch-to-server application. MultiLink Trunking provides media and module redundancy.

## MultiLink Trunk (MLT) features

A number of Nortel Networks products implement MultiLink Trunking and have different features and requirements based on the architecture of the device. For the BayStack 420/425, MultiLink Trunking has the following general features and requirements:

- A unit can have up to six MultiLink Trunks (MLTs).
- Up to four ports can belong to an MLT.
- The ports must be in the same unit in the stack.
- MultiLink Trunking is supported on 10BASE-T and 100BASE-TX ports.
- MultiLink Trunking is compatible with the Spanning Tree Protocol.
- IEEE 802.1Q tagging is supported on an MLT.
- For bridge traffic, the algorithm that distributes traffic across an MLT is based on the source and destination MAC addresses.

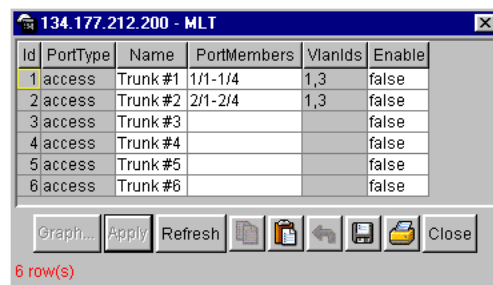
## Setting up MLTs

To set up MLTs:

- ➡ From the Device Manager menu bar, choose VLAN > MLT.

The MLT dialog box opens (Figure 51).

**Figure 51** MLT dialog box



The active MultiLink Trunks are displayed with the fields described in Table 42.

**Table 42** MLT dialog box fields

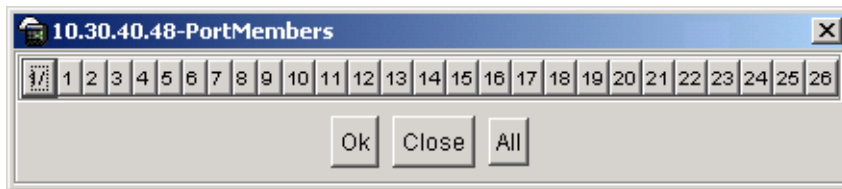
Field	Description
ID	The number of the MLT (assigned consecutively).
Name	The name given to the MLT.
PortType	Access or trunk port.
PortMembers	The ports that are assigned to the MLT.
VLANIDs	The VLANs assigned to the MLT
Enable	Specifies enabling of the MLT.

## Adding ports to a MultiLink Trunk

To add ports to an existing MLT:

- 1 From the Device Manager menu bar, choose VLAN > MLT.  
The MLT dialog box opens ([Figure 51 on page 118](#)).
- 2 Double-click the PortMembers field.  
The PortMembers dialog box opens ([Figure 52](#)).

**Figure 52** PortMembers dialog box



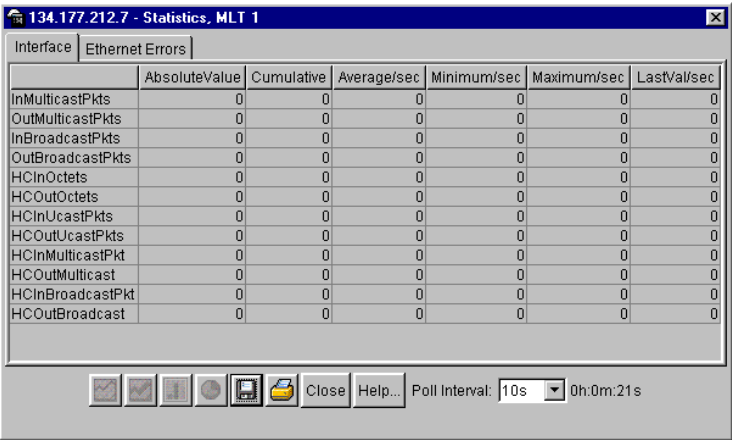
- 3 Click the port numbers you want to add.
- 4 Click OK.
- 5 In the Enable column, select True to enable your selection.

## MultiLink Trunk statistics

To view MLT interface statistics:

- 1 From the Device Manager menu bar, choose VLAN > MLT.  
The MLT dialog box opens ([Figure 51 on page 118](#)).
- 2 Select an MLT row and then click Graph.  
The Statistics, MLT window ([Figure 53](#)) opens with the Interface tab displayed.

**Figure 53** MLT Statistics — Interface tab



	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
InMulticastPkts	0	0	0	0	0	0
OutMulticastPkts	0	0	0	0	0	0
InBroadcastPkts	0	0	0	0	0	0
OutBroadcastPkts	0	0	0	0	0	0
HCInOctets	0	0	0	0	0	0
HCOctets	0	0	0	0	0	0
HCInUcastPkts	0	0	0	0	0	0
HCOUcastPkts	0	0	0	0	0	0
HCInMulticastPkt	0	0	0	0	0	0
HCOmulticast	0	0	0	0	0	0
HCInBroadcastPkt	0	0	0	0	0	0
HCOBroadcast	0	0	0	0	0	0

Table 43 describes the fields in the Interface tab.

**Table 43** Interface tab fields

Field	Description
InMulticastPkt	The number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
OutMulticast	The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
InBroadcastPkt	The number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
OutBroadcast	The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.



## MultiLink Trunk Ethernet error statistics

To view MultiLink Trunk Ethernet error statistics:

- 1 From the Device Manager menu bar, choose VLAN > MLT.

The MLT dialog box opens (Figure 51 on page 118).

- 2 Select an MLT by clicking anywhere within a field in the row.
- 3 Click Graph.

The Statistics, MLT dialog box opens (Figure 53 on page 120) with the Interface tab displayed.

- 4 Click the Ethernet Errors tab.

The Ethernet Errors tab opens (Figure 54).

**Figure 54** MLT Statics dialog box — Ethernet Errors tab

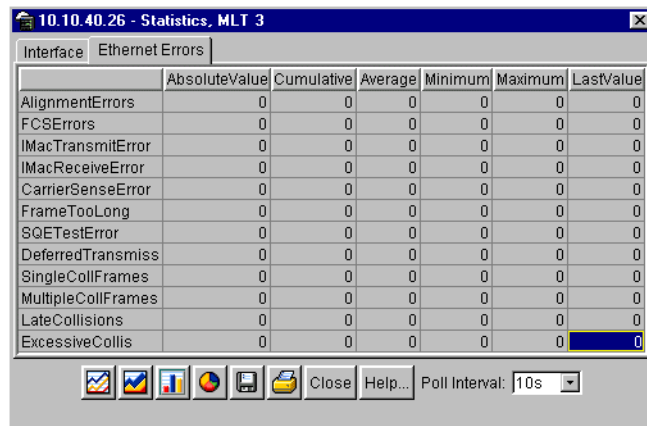


Table 44 describes the fields in the Ethernet Errors tab.

**Table 44** Ethernet Errors tab fields

Field	Description
AlignmentErrors	A count of frames received on a particular MLT that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	A count of frames received on an MLT that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
IMacTransmitError	A count of frames for which transmission on a particular MLT fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.
IMacReceiveError	A count of frames for which reception on a particular MLT fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object.  The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.
CarrierSenseErrors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular MLT. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.

**Table 44** Ethernet Errors tab fields (continued)

Field	Description
FrameTooLong	A count of frames received on a particular MLT that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
SQETestError	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular MLT. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
DeferredTransmiss	A count of frames for which the first transmission attempt on a particular MLT is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollFrames	A count of successfully transmitted frames on a particular MLT for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollFrames	A count of successfully transmitted frames on a particular MLT for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	The number of times that a collision is detected on a particular MLT later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveColls	A count of frames for which transmission on a particular MLT fails due to excessive collisions.



---

## Chapter 5

# Creating and managing VLANs

---

This chapter describes using Device Manager to manage VLANs on your BayStack 420/425 Switch. The chapter covers creating, editing, and deleting VLANs. It includes the following sections:

- VLANs (next)
- [Creating VLANs \(page 126\)](#)
- [Modifying and managing existing VLANs \(page 130\)](#)

## VLANs

A VLAN is a collection of ports on one or more switches that define a broadcast domain. The Baystack 420/425 switch supports port-based VLANs.

For a further description of VLANs, refer to *Using the BayStack 425 10/100/1000 Switch*.

When you create VLANs using Device Manager, observe the following rules:

- The ports in a VLAN or MLT must be a subset of a single spanning tree group.
- VLANs must have unique VLAN IDs and names.

## Creating VLANs

Device Manager enables you to create a port-based VLAN.

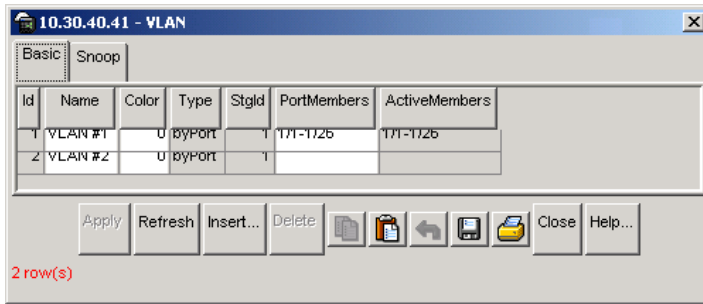
### VLAN Information

To open the VLAN dialog box:

- From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens ([Figure 55](#)).

**Figure 55** VLAN - Basic dialog box



[Table 45](#) describes the VLAN - Basic dialog box fields.

**Table 45** VLAN dialog box fields

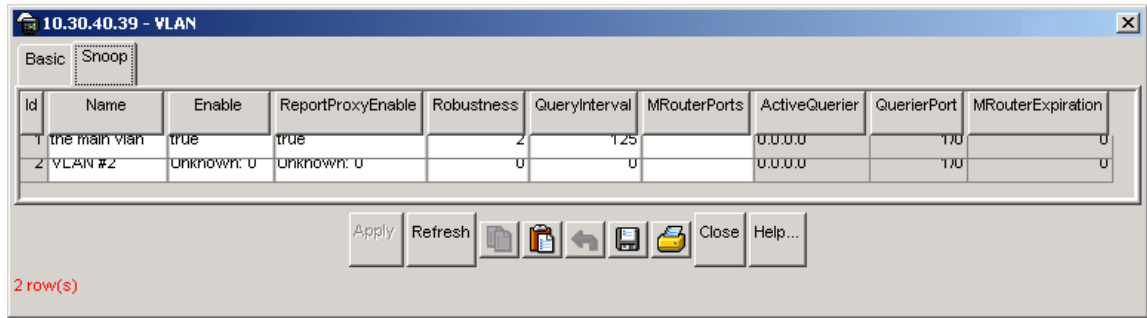
Field	Description
Id	The VLAN ID for the VLAN (unlabeled farthest left column).
Name	Name of the VLAN.
Color	An administratively-assigned color code for the VLAN. The value of this object is used by the VLAN Manager GUI tool to select a color when it draws this VLAN on the screen.
Type	Indicates the type of VLAN: byPort or byProtocolId.
StgId	Spanning tree group ID to which the VLAN belongs.
PortMembers	Ports that are members of the VLAN.
ActiveMember	Set of ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met.

To open the VLAN - Snoop dialog box:

- In the VLAN - Basic dialog box, click on the Snoop tab.

The VLAN - Snoop dialog box ([Figure 56](#)) opens.

**Figure 56** VLAN dialog box- Snoop tab



[Table 46](#) describes the VLAN - Snoop dialog box fields.

**Table 46** VLAN - Snoop dialog box fields

Field	Description
ID	Specifies the VLAN identifier.
Name	Specifies the name of the VLAN
Enable	Specifies the enable status of the VLAN
ReportProxyEnable	Specifies that ReportProxy is enabled.
Robustness	Specifies the level of robustness.
QueryInterval	Specifies the interval between queries.
MRouterports	Specifies the MRouterports.
ActiveQuerier	Specifies the active querier.
Querierport	Specifies the querier port.
MRRouterExpiration	Specifies the MRrouter expiration.

## Creating a port-based VLAN

To create a port-based VLAN:

- 1 From the Device Manager menu bar, choose VLAN > VLANs.

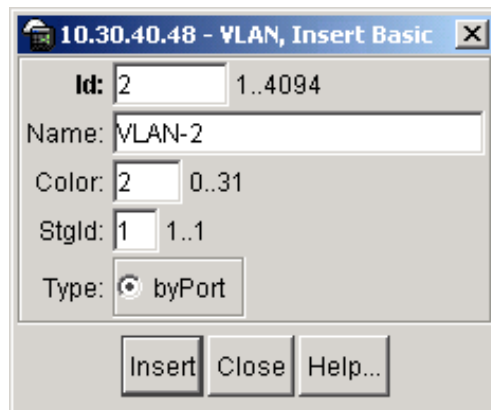
The VLAN dialog box opens ([Figure 55 on page 126](#)).

- 2 Click Insert.

The VLAN Insert Basic dialog box for creating VLANs opens ([Figure 57](#)).

This dialog box opens with the Type field set to byPort.

**Figure 57** VLAN, Insert Basic dialog box for a port-based VLANs



- 3 Type the VLAN ID.

The value can be from 1 to 4094, as long as it is not already in use. (The default VLAN has a VID=1.)

- 4 Type the VLAN name (optional).

If no name is entered, a default name is created.

- 5 In the Type field, click byPort if not already selected.

- 6 Specify the port membership by clicking the PortMembers buttons.

- 7 Click Insert.



## Accepting untagged frames

In the BayStack 420/425, you configure whether or not untagged frames are sent or received on the port level. Refer to [“VLAN tab for a single port” on page 88](#) for VLAN tab field descriptions. You can select whether or not to discard untagged frames received on a port:

The default is not to discard the untagged frames. You can also designate the port-based VLAN to which these frames are assigned by setting the untagged port's default VID (the default is 1).

To set a port to discard untagged frames it receives:

- 1 In the Device Manager main window, select a port.
- 2 From the Device Manager menu bar, choose Edit > Port.

The Port dialog box opens with the Interface tab displayed ([Figure 38 on page 86](#)).

- 3 Click the VLAN tab.

The VLAN tab opens ([Figure 58](#)).

**Figure 58** VLAN tab



Select the DiscardTaggedFrames and the DiscardUntaggFrames check boxes.

- 4 Click Apply.

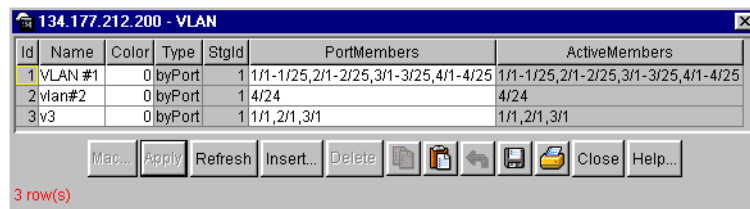
## Modifying and managing existing VLANs

The main dialog box for managing VLANs in Device Manager is the VLAN dialog box. To open the VLAN dialog box:

- From the Device Manager main menu, choose VLAN > VLANs.

The VLAN dialog box opens (Figure 59). The VLAN dialog box displays all defined VLANs, their configurations, and their current status.

**Figure 59** VLAN dialog box



**Note:** After a VLAN is created, you cannot change the VLAN type. The VLAN must be deleted and a new VLAN of the chosen type created.

Table 47 describes the fields in the VLAN dialog box.

**Table 47** VLAN dialog box fields

Field	Description
Id	The VLAN ID for the VLAN (unlabeled farthest left column).
Name	The name of the VLAN.
Color	The color used, for visual purposes only, by VLAN Manager to associate a color with a VLAN. The assigned color does not affect the behavior of a frame, only the attributes assigned to the VLAN.
Type	Indicates the type of VLAN: byPort.
StgId	The spanning tree group ID to which the VLAN belongs.
PortMembers	The ports that are members of the VLAN.
ActiveMembers	Set of ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met.

## Chapter 6

# Setting up bridging

---

The Bridge parameters allow you to configure the global Spanning Tree and to view MAC address table for a Baystack 420/425. Bridge information also includes Spanning Tree Group (STG) information.

This chapter describes the bridge information available in Device Manager on the following tabs:

- Base tab (next)
- Spanning tree tab (page 132)
- Transparent tab (page 135)
- Forwarding (page 136)
- Configuration tab (page 139)
- Status tab (page 140)
- Port tab (page 142)

### Base tab

The MAC address used by the bridge must be referred to in a unique fashion; moreover, it should be the smallest MAC address (numerically) of all ports that belong to the bridge. However it is only required to be unique when integrated with dot1dStpPriority. A unique BridgeIdentifier is formed that is used in the Spanning Tree Protocol.

To view the Base tab:

➔ From the menu bar, select Edit > Bridge.

The Bridge dialog box opens with the Base tab displayed (Figure 60).

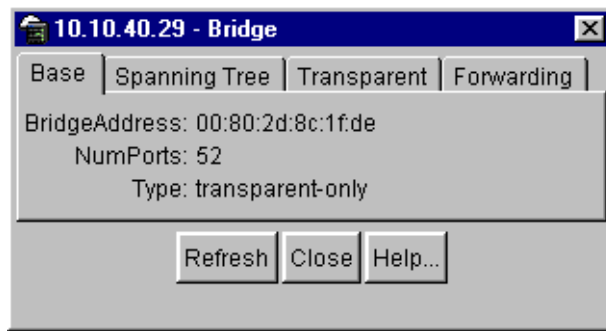
**Figure 60** Base tab

Table 48 describes the Base tab fields.

**Table 48** Base tab fields

Field	Description
BridgeAddress	MAC address of the bridge when it is referred to in a unique fashion. This address should be the smallest MAC address of all ports that belong to the bridge. However, it is has to be unique. When concatenated with dot1dStpPriority, a unique bridge ID is formed that is then used in the Spanning Tree Protocol.
NumPorts	Number of ports controlled by the bridging entity.
Type	Indicates the type of bridging this bridge can perform. If the bridge is actually performing a certain type of bridging, this will be indicated by entries in the port table for the given type.

## Spanning Tree tab

The Spanning Tree tab displays the version of the spanning tree protocol currently running. If future versions of the IEEE spanning tree protocol are released that are incompatible with the current version, a new value will be defined.

To view the Spanning Tree tab:

- 1 From the Device Manager menu bar, choose Edit > Bridge.  
The Bridge dialog box opens, with the Base tab displayed (Figure 61).
- 2 Click the Spanning Tree tab.  
The Spanning Tree tab opens.

Figure 61 Spanning Tree tab

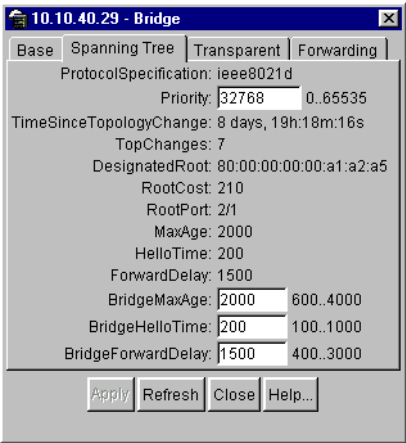


Table 49 describes the Spanning Tree tab fields.

Table 49 Spanning Tree tab fields

Field	Description
ProtocolSpecification	Version of the Spanning Tree Protocol being run. Values include: <ul style="list-style-type: none"><li>• decLb100: Indicates the DEC LANbridge 100 Spanning Tree Protocol.</li><li>• ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value will be defined.</li></ul>
Priority	Value of the writable portion of the bridge ID. That is, the first two octets of the (8-octet long) bridge ID. The last six octets of the bridge ID are given by the value of BridgeAddress.
TimeSinceTopologyChange	Time (in hundredths of a second) since the last time a topology change was detected by the bridge entity.
TopChanges	Number of topology changes detected by this bridge since the management entity was reset or initialized.
DesignatedRoot	Bridge ID of the root of the spanning tree as determined by the Spanning Tree Protocol. This is executed by the node. This value is used as the Root ID parameter in all configuration bridge PDUs originated by the node.

**Table 49** Spanning Tree tab fields (continued)

Field	Description
RootCost	Cost of the path to the root as seen from this bridge.
RootPort	Port number of the port that offers the lowest cost path from this bridge to the root bridge.
MaxAge	Maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using.
HelloTime	Time between the transmission of Configuration bridge PDUs by the node on any port when it is the root of the spanning tree (in units of hundredths of a second). This is the actual value that the bridge is currently using.
ForwardDelay	<p>Value (in hundredths of a second) that controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, that precede the Forwarding state. The value is also used when a topology change has been detected and is underway. This ages all dynamic entries in the Forwarding database.</p> <p><b>Note:</b> This value is the one that this bridge is currently using, in contrast to dot1dStpBridge ForwardDelay which is the value that this bridge and all others would start using if/when this bridge were to become the root.]</p>
BridgeMaxAge	<p>Value that all bridges use for the maximum age of a bridge when it is acting as the root.</p> <p><b>Note:</b> 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.</p>

**Table 49** Spanning Tree tab fields (continued)

Field	Description
BridgeHelloTime	Value that the bridge uses for HelloTime when the bridge is acting as the root. The granularity of this timer is specified by 802.1D-1990 to be one second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds.
TimeSinceTopologyChange	Value that all bridges use for ForwardDelay when this bridge is acting as the root.  Note: 802.1D-1990 specifies that the range for this parameter is related to the value of dot1dStpBridgeMaxAge. The granularity of this timer is specified by 802.1D-1990 to be one second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds.

## Transparent tab

The Transparent tab contains information about a specific unicast MAC address that has forwarding information for the bridge.

To view the Transparent tab:

- 1 From the Device Manager menu bar, choose Edit > Bridge.  
The Bridge dialog box opens, with the Base tab displayed.
- 2 Click the Transparent tab.  
The Transparent tab opens (Figure 62).

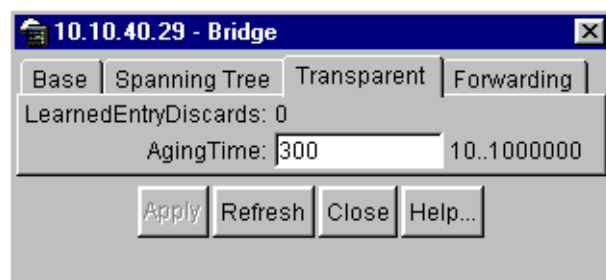
**Figure 62** Transparent tab

Table 50 describes the Transparent tab items.

**Table 50** Transparent tab items

Item	Description
LearnedEntryDiscard	Number of Forwarding database entries learned that have been discarded due to a lack of space in the Forwarding database. If this counter is increasing, it indicates that the Forwarding database is becoming full regularly. This condition will effect the performance of the subnetwork. If the counter has a significant value and is not presently increasing, it indicates that the problem has been occurring but is not persistent.
AgingTime	Time-out period in seconds for aging out dynamically learned forwarding information. <b>Note:</b> The 802.1D-1990 specification recommends a default of 300 seconds.

## Forwarding tab

The Forwarding tab displays the current state of the port, as defined by application of the Spanning Tree Protocol. This state controls what action a port takes when a frame is received. If the bridge detects a port that is malfunctioning, it places the port into the “broken” state. For ports that are disabled, the value is “disabled.”

To view the Forwarding tab:

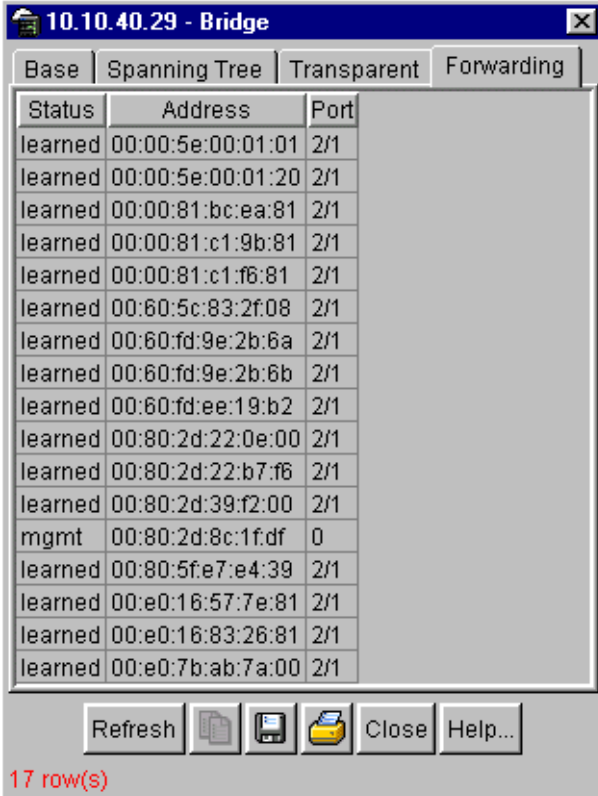
- 1 From the Device Manager menu bar, choose Edit > Bridge.

The Bridge dialog box opens, with the Base tab displayed.

- 2 Click the Forwarding tab.

The Forwarding tab opens (Figure 63).



**Figure 63** Forwarding tab

Status	Address	Port
learned	00:00:5e:00:01:01	2/1
learned	00:00:5e:00:01:20	2/1
learned	00:00:81:bc:ea:81	2/1
learned	00:00:81:c1:9b:81	2/1
learned	00:00:81:c1:f6:81	2/1
learned	00:60:5c:83:2f:08	2/1
learned	00:60:fd:9e:2b:6a	2/1
learned	00:60:fd:9e:2b:6b	2/1
learned	00:60:fd:ee:19:b2	2/1
learned	00:80:2d:22:0e:00	2/1
learned	00:80:2d:22:b7:f6	2/1
learned	00:80:2d:39:f2:00	2/1
mgmt	00:80:2d:8c:1f:df	0
learned	00:80:5f:e7:e4:39	2/1
learned	00:e0:16:57:7e:81	2/1
learned	00:e0:16:83:26:81	2/1
learned	00:e0:7b:ab:7a:00	2/1

17 row(s)

Table 51 describes the Forwarding tab fields.

**Table 51** Forwarding tab fields

Field	Description
Status	<p>The values of this fields include:</p> <ul style="list-style-type: none"> <li>invalid: Entry is no longer valid, but has not been removed from the table.</li> <li>learned: Value of the corresponding instance of dot1dTpFdbPort was learned and is being used.</li> <li>self: Value of the corresponding instance of dot1dTpFdbAddress represents an address of the bridge. The corresponding instance of dot1dTpFdbPort indicates that a specific port on the bridge has this address.</li> <li>mgmt(5): Value of the corresponding instance of dot1dTpFdbAddress is also the value of an existing instance of dot1dStaticAddress.</li> <li>other: none of the preceding. This would include where some other MIB object (not the corresponding instance of dot1dTpFdbPort or an entry in the dot1dStaticTable) is being used to determine if a frames addressed to the value of dot1dTpFdbAddress are being forwarded.</li> </ul>
Address	A unicast MAC address for which the bridge has forwarding or filtering information.
Port	<p>Either the value “0” or the port number on a frame has been seen. The source address must be equal to the value of the corresponding instance of dot1dTpFdbAddress</p> <p>A value of “0” indicates that the port number has not been learned, so the bridge does have the forwarding/filtering information for this address (located in the dot1dStaticTable). You should assign the port value to this object whenever it is learned even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned(3).</p>

## Spanning tree group (STG)

The spanning tree group (STG) information is stored in the STG dialog box. Each row in each tab specifies a different STG in the device.

## Configuration tab

The Configuration tab in the STG dialog box has general information for the STG.

To view the Configuration tab:

➔ From the Device Manager menu bar, choose VLANs > STG.

The STG dialog box opens, with the Configuration tab displayed (Figure 64).

**Figure 64** Configuration tab

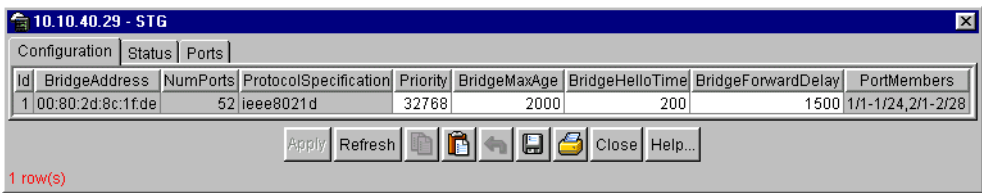


Table 52 describes the Configuration tab fields.

**Table 52** Configuration tab fields

Item	Description
ID	An identifier used to identify a STG in the device.
BridgeAddress	MAC address used by a bridge when it is referred to in a unique fashion. Nortel Network recommends that the number be the smallest MAC address of all ports belonging to the bridge. However, it is only required to be unique. When concatenated with Priority, a unique bridge identifier is formed that is used in the Spanning Tree Protocol.
NumPorts	Number of ports controlled by this bridging entity.
ProtocolSpecification	Version of the spanning tree protocol being run. Values include: <ul style="list-style-type: none"><li>• decLb100: Indicates the DEC LANbridge 100 Spanning Tree Protocol.</li><li>• ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value will be defined.</li></ul>
Priority	Value of the writable portion of the bridge ID. That is, the first two octets of the (8-octet long) bridge ID. The last six octets of the bridge ID are given by the value of BridgeAddress.

**Table 52** Configuration tab fields (continued)

Item	Description
BridgeMaxAge	Value that all bridges use for the maximum age of a bridge when it is acting as the root. <b>Note:</b> 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.
BridgeHelloTime	Value that all bridges use for HelloTime when a bridge is acting as the root. <b>Note:</b> The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.
BridgeForwardDelay	Value that all bridges use for ForwardDelay when this bridge is acting as the root. <b>Note:</b> 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.
PortMembers	Bit-field used to identify the ports in the system that are members this STG. The bit-field is 32 octets long representing ports 0 to 255 (inclusive).

## Status tab

The Status tab in the STG dialog box has status information for the STG.

To view the Status tab:

- 1 From the Device Manager menu bar, choose VLANs > STG.

The STG dialog box opens, with the Configuration tab displayed.

- 2 Click the Status tab.

The Status tab opens (Figure 65).

Figure 65 Status tab

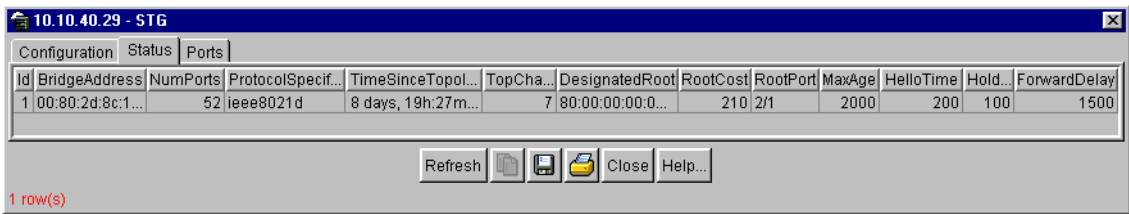


Table 53 describes the Status tab fields.

Table 53 Status tab fields

Field	Description
ID	An identifier used to identify a STG in the device.
BridgeAddress	MAC address used by a bridge when it is referred to in a unique fashion. Nortel Networks recommends that the number be the smallest MAC address of all ports belonging to the bridge. However, it is only required to be unique. When concatenated with Priority, a unique bridge identifier is formed that is used in the Spanning Tree Protocol.
NumPorts	Number of ports controlled by this bridging entity.
ProtocolSpecification	Version of the Spanning Tree Protocol being run. Values include: <ul style="list-style-type: none"><li>• decLb100: Indicates the DEC LANbridge 100 spanning tree protocol.</li><li>• ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE spanning tree protocol are released that are incompatible with the current version, a new value will be defined.</li></ul>
TimeSinceTopologyChange	Time (in hundredths of seconds) since the last topology change was detected by the bridge entity.
TopChange	Number of topology changes detected by the bridge since the management entity was last reset or initialized.
DesignatedRoot	Bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol. The value is used as the root identifier parameter in all configuration bridge PDUs originated by this node.
RootCost	Cost of the path to the root as seen from the bridge.
RootPort	Port that has the lowest cost path from the bridge to the root bridge.

**Table 53** Status tab fields (continued)

Field	Description
MaxAge	Maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using.
HelloTime	Amount of time between the transmission of configuration bridge PDUs by this node on any port when it is the root of the spanning tree (in hundredths of a seconds). This is the actual value that this bridge is currently using.
HoldTime	Value of the interval length during which no more than two configuration bridge PDUs shall be transmitted by this node (in hundredths of a second).
ForwardDelay	<p>This time value (in hundredths of a seconds) that controls how fast a port changes its spanning state when moving towards the forwarding state.</p> <p>Value determines how long the port stays in each of the listening and learning states, which precede the forwarding state. This is also used when a topology change has been detected and is underway, to age all dynamic entries in the forwarding database.</p> <p><b>Note:</b> This value is the one that this bridge is currently using, in contrast to BridgeForwardDelay which is the value that this bridge and all others would start using if/when this bridge were to become the root.</p>

## Ports tab

The Ports tab in the STG dialog box has port information for the STG.

To view the Ports tab:

- 1 From the Device Manager menu bar, choose VLANs > STG.

The STG dialog box opens, with the Configuration tab displayed.

- 2 Click the Ports tab.

The Ports tab opens (Figure 66).

Figure 66 Ports tab

	StgId	Priority	State	EnableStp	FastStart	PathCost	DesignatedRoot	DesignatedCost	DesignatedBridge	DesignatedPort	ForwardTransitions
1/1	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:01	6
1/2	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:02	3
1/3	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:03	4
1/4	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:04	1
1/5	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:05	1
1/6	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:06	1
1/7	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:07	1
1/8	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:08	1
1/9	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:09	1
1/10	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:0a	1
1/11	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:0b	1
1/12	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:0c	1
1/13	1	128	forwardi...	true	true	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:0d	1
1/14	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:0e	1
1/15	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:0f	1
1/16	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:10	1
1/17	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:11	1
1/18	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:12	1
1/19	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:13	1
1/20	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:14	1
1/21	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:15	1
1/22	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:16	1
1/23	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:17	1
1/24	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:18	1
2/1	1	128	forwardi...	true	false	10	80:00:00:00:00:...	200	80:00:00:60:fd:9...	80:2c	1
2/2	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:22	1

52 row(s)

Table 54 describes the Ports tab fields.

Table 54 Ports tab fields

Field	Description
StgId	STG identifier assigned to this port.
Priority	Value of the priority field contained in the first octet of the port ID. The other octet is given by the value of the “rcStgPort.”
State	The current state of the port as defined by application of the Spanning Tree Protocol. These are the instructions the port takes on a frame when it is received. If the bridge detects a port is malfunctioning, it will list it as “broken(6).” For ports that are disabled, the value is “disabled(1).”
EnableStp	Enables (True) or disables (False) the spanning tree of the port.
FastStart	When this is enabled (True), the port is move to forwarding or blocking state in 4 seconds.

**Table 54** Ports tab fields (continued)

Field	Description
PathCost	Contribution of the port to the pathcost of paths towards the spanning tree root, including the current port. 802.1D-1990 specifications recommends that the default of this parameter be in inverse proportion to the speed of the attached LAN.
DesignatedRoot	The unique "Bridge Identifier." This is recorded as Root in the configuration bridge PDUs transmitted by the Designated Bridge for the segment to that the port is attached.
DesignatedCost	Path cost of the Designated Port of the segment connected to the port. The value is compared to the Root Path Cost field in received bridge PDUs.
DesignatedBridge	Bridge identifier of the bridge that this port considers to be the Designated Bridge for this port's segment.
DesignatedPort	Port identifier of the port on the Designated Bridge for this port's segment.
ForwardTransitions	Number of times this port has transitioned from the learning state to the forwarding state.



---

## Chapter 7

# Troubleshooting Device Manager

---

This chapter describes diagnostic information available in Device Manager on the following tabs:

- [Topology tab](#) (next)
- [Topology Table tab](#) (page 146)

## Topology tab

To view topology information:

- ➔ From the Device Manager menu bar, select Edit > Diagnostics.

The Diagnostics dialog box opens with the Topology tab displayed ([Figure 67](#)).

**Figure 67** Diagnostics dialog box — Topology tab

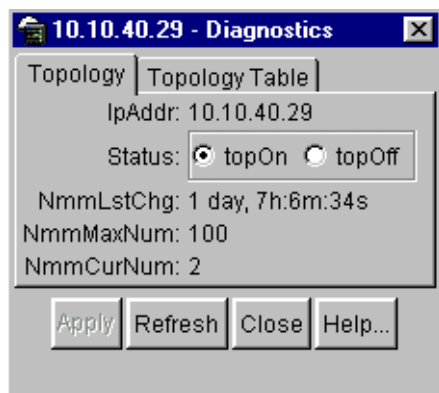


Table 55 describes the Topology tab items.

**Table 55** Topology tab items

Items	Description
IpAddr	The IP address of the device.
Status	Whether Nortel Networks topology is on (topOn) or off (topOff) for the device. The default value is topOn.
NmmLstChg	The value of sysUpTime the last time an entry in the network management MIB (NMM) topology table was added, deleted, or modified. If the table has not changed since the last cold or warm start of the agent.
NmmMaxNum	The maximum number of entries in the NMM topology table.
NmmCurNum	The current number of entries in the NMM topology table.

## Topology Table tab

To view more topology information:

- 1 From the Device Manager menu bar, choose Edit > Diagnostics.  
The Diagnostics dialog box opens with the Topology tab displayed (Figure 67 on page 145).
- 2 Click the Topology Table tab.  
The Topology Table tab opens (Figure 68).

**Figure 68** Diagnostics dialog box — Topology Table tab

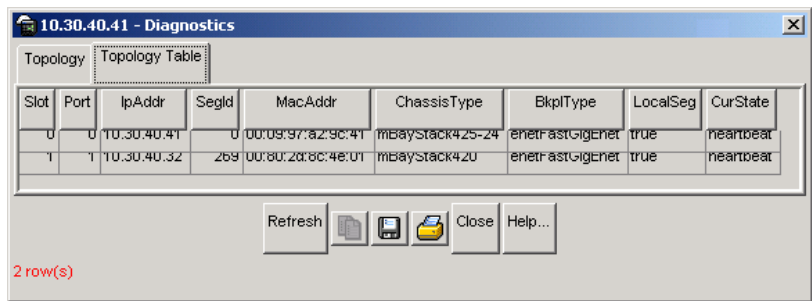


Table 56 describes the Topology Table tab fields.

**Table 56** Topology Table tab fields

Field	Description
Slot	The slot number in the chassis in which the topology message was received.
Port	The port on which the topology message was received.
IpAddr	The IP address of the sender of the topology message.
SegId	The segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message.
MacAddr	The MAC address of the sender of the topology message.
ChassisType	The chassis type of the device that sent the topology message.
BkplType	The backplane type of the device that sent the topology message.
LocalSeg	Indicates if the sender of the topology message is on the same Ethernet segment as the reporting agent.
CurState	The current state of the sender of the topology message. The choices are: <ul style="list-style-type: none"><li>• topChanged —Topology information has recently changed.</li><li>• heartbeat —Topology information is unchanged.</li><li>• new — The sending agent is in a new state.</li></ul>



---

## Chapter 8

# RMON

---

The Remote Network Monitoring (RMON) MIB is an interface between the RMON agent on a Baystack 420/425 Switch and an RMON management application, such as the Device Manager. It defines objects that are suitable for the management of any type of network, but some groups are targeted for Ethernet networks in particular. The RMON agent continuously collects statistics and proactively monitors switch performance. You can view this data through the Device Manager.

RMON has three major functions:

- Creating and displaying alarms for user-defined events
- Gathering cumulative statistics for Ethernet interfaces
- Tracking a history of statistics for Ethernet interfaces

## Working with RMON information

You can view RMON information by looking at the Graph information associated with the port or chassis.

### Viewing statistics

Device Manager gathers Ethernet statistics that you can have graphed in a variety of formats, or you can save them to a file and export the statistics to an outside presentation or graphing application.

To view RMON Ethernet statistics:

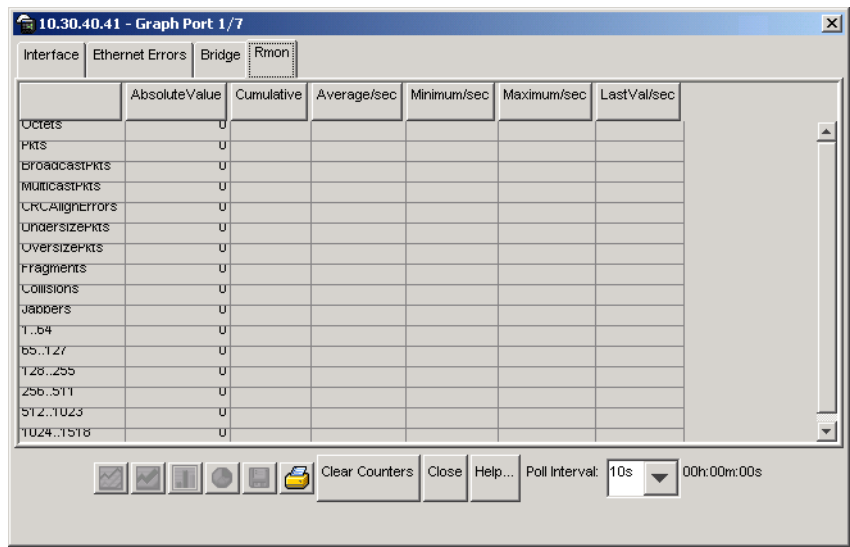
- 1 Select an object (port).

- 2 Do one of the following:
- Double-click on the selected port
  - From the shortcut menu, choose Graph.
  - From the Device Manager main menu, choose Graph.

The Graph Port dialog box opens with the Interface tab displayed (Figure 38 on page 86).

- 3 Click the RMON tab.
- The RMON tab opens (Figure 69).

**Figure 69** Port dialog box — RMON tab



For descriptions of the RMON tab fields, refer to Table 40 on page 112. For descriptions of the statistics columns, refer to Table 10 on page 39.

## Viewing history

Ethernet history records periodic statistical samples from a network. A sample is called a history and is gathered in time intervals referred to as “buckets.” Histories establish a time-dependent method for gathering RMON statistics on a port. The default values for history are:

- Buckets are gathered at 30-minute intervals.
- Number of buckets gathered is 50.

Both the time interval and the number of buckets is configurable. However, when the last bucket is reached, bucket 1 is dumped and “recycled” to hold a new bucket of statistics. Then bucket 2 is dumped, and so forth.

To view RMON history:

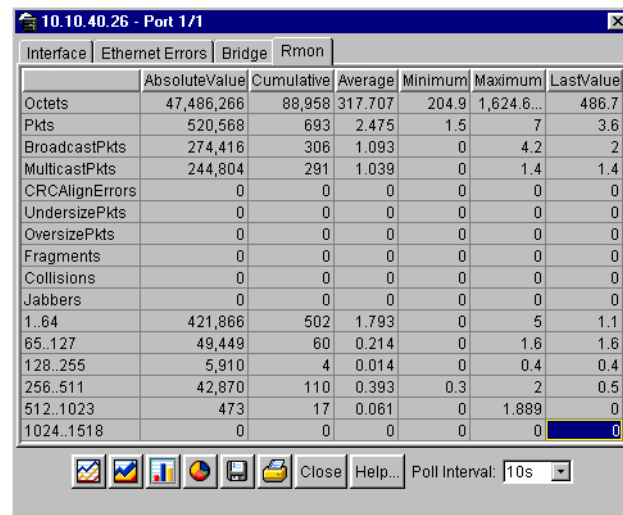
- 1 Select an object (port or chassis).
- 2 On the toolbar, click Graph.

The graph Port dialog box opens with the Interface tab displayed ([Figure 45 on page 104](#)).

- 3 Click the RMON tab.

The RMON tab opens ([Figure 70](#)).

**Figure 70** Port dialog box — RMON tab



# Creating a history

You can use RMON to collect statistics at intervals. For example, if you want RMON statistics to be gathered over the weekend, you will want enough buckets to cover two days. To do this, set the history to gather one bucket each hour, thus covering a 48-hour period. After you set history characteristics, you cannot modify them; you must delete the history and create another one.

To establish a history for a port and set the bucket interval:

- 1 From the Device Manager main menu, choose RMON > Control.  
The RMONControl dialog box opens with the History tab displayed (Figure 71).

Figure 71 History tab

Index	Port	BucketsRequested	BucketsGranted	Interval	Owner
1	1/1	3	3	30	monitor
2	1/2	3	3	30	monitor
3	1/3	3	3	30	monitor
4	1/4	3	3	30	monitor
5	1/5	3	3	30	monitor
6	1/6	3	3	30	monitor
7	1/7	3	3	30	monitor
8	1/8	3	3	30	monitor
9	1/9	3	3	30	monitor
10	1/10	3	3	30	monitor
11	1/11	3	3	30	monitor
12	1/12	3	3	30	monitor
13	1/13	3	3	30	monitor
14	1/14	3	3	30	monitor

Table 57 describes the History fields.

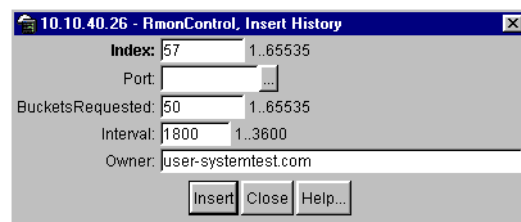


**Table 57** History tab fields

Field	Description
Index	A unique value assigned to each interface. An index identifies an entry in a table.
Port	Any Ethernet interface on the device.
BucketsRequested	The requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this entry.
BucketsGranted	The number of discrete sampling intervals over which data is saved in the part of the media-specific table associated with this entry. There are instances when the actual number of buckets associated with this entry is less than the value of this object. In this case, at the end of each sampling interval, a new bucket is added to the media-specific table.
Interval	The interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this entry. You can set this interval to any number of seconds between 1 and 3600 (1 hour). Because the counters in a bucket may overflow at their maximum value with no indication, note the possibility of overflow in any of the associated counters. It is important to consider the minimum time in which any counter could overflow on a particular media type and set the historyControlInterval object to a value less than this interval. This is typically most important for the 'octets' counter in any media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter could overflow in about one hour at the Ethernet's maximum utilization.
Owner	The network management system that created this entry.

**2** Select an index and then click Insert.

The RMONControl, Insert History dialog box opens ([Figure 72](#)).

**Figure 72** RMONControl, Insert History dialog box

- 3** Select the port from the port list or type the port number.
- 4** Set the number of buckets.  
The default is 50.
- 5** Set the interval.  
The default is 1800 seconds.
- 6** Type the owner, the network management system that created this entry.
- 7** Click Insert.  
RMON collects statistics using the index, port, bucket, and interval that you specified.

## Disabling history

To disable RMON history on a port:

- 1** From the Device Manager main menu, choose RMON > Control.  
The RMONControl dialog box opens with the History tab displayed ([Figure 71 on page 152](#)).
- 2** Highlight the row that contains the port ID you want to delete.
- 3** Click Delete.  
The entry is removed from the table.

## Enabling Ethernet statistics gathering

You can use RMON to gather Ethernet statistics.

To gather Ethernet statistics:

- 1 From the Device Manager main menu, choose RMON > Control.  
The RMONControl dialog box opens with the History tab displayed (Figure 71 on page 152).
- 2 Click the Ether Stats tab.  
The Ether Stats tab opens (Figure 73).

**Figure 73** RMONControl dialog box — Ether Stats tab

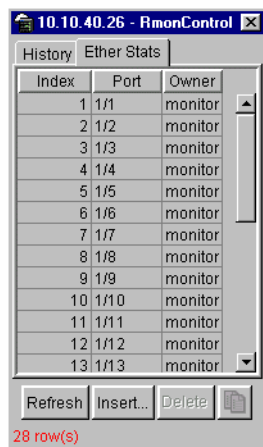


Table 58 describes the Ether Stats tab fields.

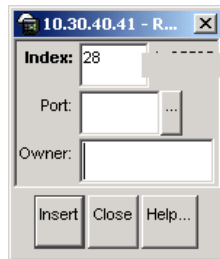
**Table 58** Ether Stats tab fields

Field	Description
Index	A unique value assigned to each interface. An index identifies an entry in a table.
Port	Any Ethernet interface on the device.
Owner	The network management system which created this entry.

**3** Click Insert.

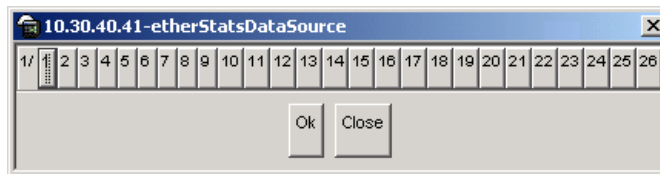
The RMONControl, Insert Ether Stats dialog box opens ([Figure 74](#)).

**Figure 74** RMONControl, Insert Ether Stats dialog box

**4** Select the port(s).

Enter the port number you want or select the port from the list menu ([Figure 75](#)).

**Figure 75** RMONControl, Insert Ether Stats dialog box port list



Device Manager assigns the index.

**5** Click Insert.

The new Ethernet Statistics entry is displayed in the Ether Stats tab.

## Disabling Ethernet statistics gathering

To disable Ethernet statistics that you have set:

**1** From the Device Manager main menu, choose RMON > Control.

The RMONControl dialog box opens with the History tab displayed ([Figure 71 on page 152](#)).

- 2 Click the Ether Stats tab.

The Ether Stats tab opens ([Figure 74 on page 156](#)).

- 3 Highlight the row that contains the port ID you want to delete.

- 4 Click Delete.

The Ether Stats entry is removed from the table.

## Alarms

Alarms are useful when you need to know when the values of a variable go out of range. You can define an RMON alarm for any MIB variable that resolves to an integer value. You cannot use string variables (such as system description) as alarm variables.

All alarms share the following characteristics:

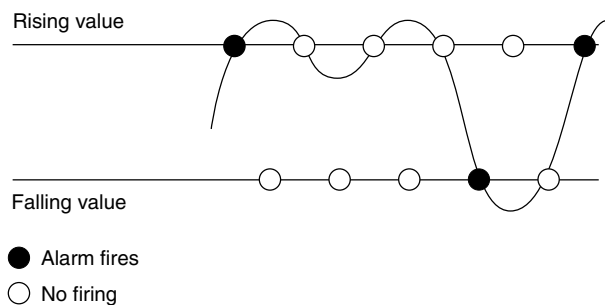
- An upper and lower threshold value is defined.
- A corresponding rising and falling event occurs.
- An alarm interval or polling period is reached.

When alarms are activated, you can view the activity in a log or a trap log, or you can create a script to notify you by beeping a console, sending e-mail, or calling a pager.

### How RMON alarms work

The alarm variable is polled and the result is compared against upper and lower limit values you select when you create the alarm. If either limit is reached or crossed during the polling period, then the alarm fires and generates an event that you can view in the event log or the trap log.

The alarm's upper limit is called the *rising value*, and its lower limit is called the *falling value*. RMON periodically samples the data based upon the alarm interval. During the *first* interval that the data passes above the rising value, the alarm fires as a rising event. During the first interval that the data drops below the falling value, the alarm fires as a falling event ([Figure 76](#)).

**Figure 76** How alarms fire

It is important to note that the alarm fires during the first interval that the sample goes out of range. No additional events are generated for that threshold until the opposite threshold is crossed. Therefore, it is important to carefully define the rising and falling threshold values for alarms to work as expected. Otherwise, incorrect thresholds causes an alarm to fire at every alarm interval.

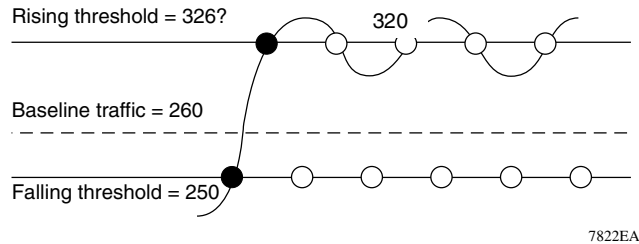
A general guideline is to define one of the threshold values to an expected, baseline value, and then define the opposite threshold as the out-of-bounds limit. Because of sample averaging, the value may be equal to  $\pm 1$  of the baseline units. For example, assume an alarm is defined on octets going out of a port as the variable. The intent of the alarm is to provide notification to the system administrator when excessive traffic occurs on that port. If spanning tree is enabled, then 52 octets are transmitted out of the port every 2 seconds, which is equivalent to baseline traffic of 260 octets every 10 seconds. This alarm should provide the notification the system administrator needs if the lower limit of octets going out is defined at 260 and the upper limit is defined at 320 (or at any value greater than  $260 + 52 = 312$ ).

The first time outbound traffic other than spanning tree Bridge Protocol Data Units (BPDUs) occurs, the rising alarm fires. When outbound traffic other than spanning tree ceases, the falling alarm fires. This process provides the system administrator with time intervals of any nonbaseline outbound traffic.

If the alarm is defined with a falling threshold less than 260 (assuming the alarm polling interval is 10 seconds), say 250, then the rising alarm can fire only once (Figure 77). The reason is that for the rising alarm to fire a second time, the falling alarm (the opposite threshold) must fire. Unless the port becomes inactive or

spanning tree is disabled (which would cause the value for outbound octets to drop to zero), the falling alarm cannot fire because the baseline traffic is always greater than the value of the falling threshold. By definition, the failure of the falling alarm to fire prevents the rising alarm from firing a second time.

**Figure 77** Alarm example — threshold less than 260



## Creating alarms

When you create an alarm, you select a variable from the variable list and a port, or other switch component, to which it is connected. Some variables require port IDs, card IDs, or other indices (for example, spanning tree group IDs). You then select a rising and a falling threshold value. The rising and falling values are compared against the actual value of the variable that you choose. If the variable falls outside of the rising or falling value range, an alarm is triggered and an event is logged or trapped.

When you create an alarm, you also select a sample type, which can be either absolute or delta. *Absolute* alarms are defined on the cumulative value of the alarm variable. An example of an alarm defined with absolute value is card operating status. Because this value is not cumulative, but instead represents states, such as card up (value 1) and card down (value 2), you set it for absolute value. Therefore, an alarm could be created with a rising value of 2 and a falling value of 1 to alert a user to whether the card is up or down.

Most alarm variables related to Ethernet traffic are set to *delta* value. Delta alarms are defined based on the difference in the value of the alarm variable between the start of the polling period and the end of the polling period. Delta alarms are sampled twice per polling period. For each sample, the last two values are added together and compared to the threshold values. This process increases precision

and allows for the detection of threshold crossings that span the sampling boundary. If you track the current values of a given delta-valued alarm and add them together, therefore, the result is twice the actual value. (This result is not an error in the software.)

## Alarm Manager example



**Note:** The example alarm described in the following procedure generates at least one alarm every five minutes. The example is intended only to demonstrate how alarms fire; it is not a useful alarm. Because of the high frequency, you may want to delete this alarm and replace it with a practical setting.

To create an alarm to receive statistics and history using default values:

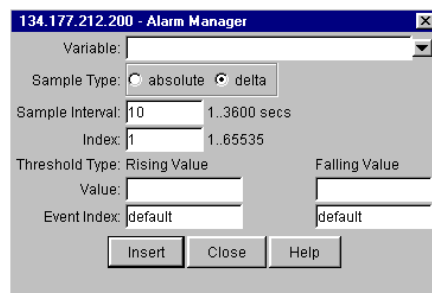
1 Do one of the following:

- From the Device Manager main menu, choose RMON >Alarm Manager.
- On the toolbar, click the Alarm Manager button.



The Alarm Manager dialog box opens ([Figure 78](#)).

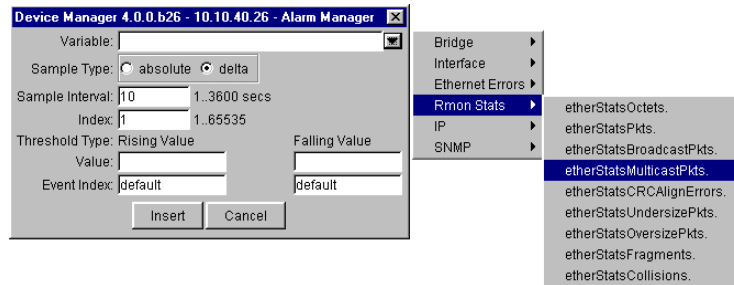
**Figure 78** Alarm Manager dialog box





- 2 In the variable field, select a variable for the alarm from the list and a port (or other ID) on which you want to set an alarm (Figure 79).

**Figure 79** Alarm variable list



Alarm variables are in three formats, depending on the type:

- A chassis alarm ends in .x where the x index is hard-coded. No further information is required.
- A card, spanning tree group (STG) or EtherStat alarm ends with a dot (.). You must enter a card number, STG ID, IP address, or EtherStat information.
- A port alarm ends with no dot or index and requires using the port shortcut menu. An example of a port alarm would be ifInOctets (interface incoming octet count).

For this example, select Bridge > dot1dStpTopChanges.0 from the variable list. This example is a chassis alarm, indicated by the “.0” in the variable.

- 3 For this example, select a rising value of 4 and a falling value of 0.
- 4 Leave the remaining fields at their default values, including a sample type of Delta. Click Insert.

If you want to make field changes, see the field descriptions shown in [Table 59](#).

**Table 59** RMON Insert Alarm dialog box fields

Field	Description	
Variable	<p>Name and type of alarm—indicated by the format: <i>alarmname.x</i> where x=0 indicates a chassis alarm.</p> <p><i>alarmname</i>. where the user must specify the index. This will be a card number for module-related alarms, an STG ID for spanning tree group alarms (the default STG is 1, other STG IDs are user-configured), or the Ether Statistics Control Index for RMON Stats alarms</p> <p><i>alarmname</i> with no dot or index is a port-related alarm and results in display of the port selection tool.</p>	
Sample Type	<p>Can be either absolute or delta.</p> <p>For more information about sample types, refer to <a href="#">“Creating alarms” on page 159</a>.</p>	
Sample Interval	Time period (in seconds) over which the data is sampled and compared with the rising and falling thresholds.	
Index	Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device.	
Threshold Type	Rising Value	Falling Value
Value	When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, generates a single event.	When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, generates a single event.
Event Index	Index of the event entry that is used when a rising threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already filled in.)	Index of the event entry that is used when a falling threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already filled in.)

To view the RMON statistics and history for the port for which you have created an alarm:

- 1 Select the port on which you have created an alarm.
- 2 From the Device Manager main menu, choose RMON > Control.

The RMONControl dialog box opens with the History tab displayed ([Figure 71 on page 152](#)).

- 3 Click the Ether Stats tab to view statistics (Figure 75 on page 156).

The RMONAlarms dialog box opens with the Alarms tab (Figure 80) displayed.

**Figure 80** RMONAlarms dialog box — Alarms tab



Table 60 describes the fields on the Alarms tab.

**Table 60** Describes the fields on the Alarms tab

Field	Description
Index	Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device
Interval	The interval in seconds over which data is sampled and compared with the rising and falling thresholds. When setting this variable, note that in the case of deltaValue sampling, you should set the interval short enough so that the sampled variable is very unlikely to increase or decrease by more than $2^{31} - 1$ during a single sampling interval.
Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Counter, Gauge, or TimeTicks) may be sampled.
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.
Value	The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value is the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value is the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and remains available until the next period completes.

**Table 60** Describes the fields on the Alarms tab (continued)

Field	Description
StartupAlarm	The alarm that may be sent when this entry is first set to valid. If the first sample after this entry becomes valid is greater than or equal to the risingThreshold and alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3), then a single rising alarm is generated. If the first sample after this entry becomes valid is less than or equal to the fallingThreshold and alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3), then a single falling alarm is generated.
RisingThreshold	A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3). After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold.
RisingEventIndex	The index of the eventEntry that is used when a rising threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is zero, no associated event is generated, because zero is not a valid event index.
FallingThreshold	A threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold and the associated alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3). After a falling event is generated, another such event is not generated until the sampled value rises above this threshold and reaches the alarmRisingThreshold.
FallingEventIndex	The index of the eventEntry that is used when a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is zero, no associated event is generated, because zero is not a valid event index.
Owner	The network management system which created this entry.
Status	The status of this alarm entry.

To delete an alarm:

- 1 From the Device Manager main menu, choose RMON > Alarms.  
The RMONAlarms dialog box opens with the Alarms tab (Figure 80) displayed.
- 2 Click any field for the alarm that you want to delete to highlight it.
- 3 Click Delete.

## Events

RMON events and alarms work together to notify you when values in your network are outside of a specified range. When values pass the specified ranges, the alarm is triggered and “fires.” The event specifies how the activity is recorded.

### How events work

An event specifies whether a trap, a log, or a trap and a log is generated to view alarm activity. When RMON is globally enabled, two default events are generated:

- RisingEvent
- FallingEvent

The default events specify that when an alarm goes out of range, the “firing” of the alarm will be tracked in both a trap and a log. For example, when an alarm fires at the rising threshold, the rising event specifies that this information be sent to both a trap and a log. Likewise, when an alarm passes the falling threshold, the falling event specifies that this information be sent to a trap and a log.

### Viewing an event

To view a table of events:

- 1 From the Device Manager main menu, choose RMON > Alarms.  
The RMONAlarms dialog box opens displaying the Alarms tab ([Figure 80 on page 163](#)).
- 2 Click the Events tab.  
The Events tab opens ([Figure 81](#)).

**Figure 81** RMONAlarms dialog box — Events tab

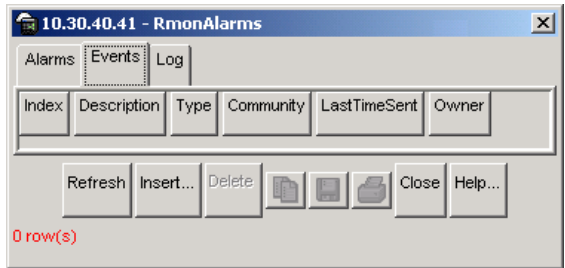


Table 61 describes the RMONAlarms Events tab fields.

**Table 61** Events tab fields

Field	Description
Index	This index uniquely identifies an entry in the event table. Each entry defines one event that is to be generated when the appropriate conditions occur.
Description	Specifies whether the event is a rising or falling event.
Type	The type of notification that the Device Manager provides about this event. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations. Possible notifications follow: <ul style="list-style-type: none"><li>• none</li><li>• log</li><li>• trap</li><li>• log-and-trap</li></ul>
Community	The SNMP community string acts as a password. Only those management applications with this community string can view the alarms.
LastTimeSent	The value of sysUpTime at the time this event entry last generated an event. If this entry has not generated any events, this value is zero.
Owner	If traps are specified to be sent to the owner, then this is the name of the machine that will receive alarm traps.

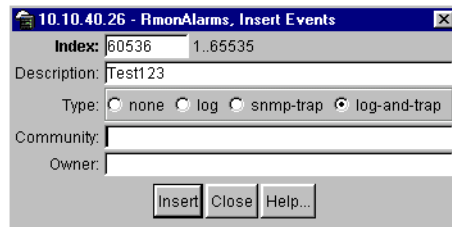
## Creating an event

To create an event:

- 1 In the RMONAlarms dialog box Events tab, click Insert.

The RMONAlarms, Insert Events dialog box opens (Figure 82).

**Figure 82** Insert Events dialog box



- 2 In the Description field, type a name for the event.
- 3 Select the type of event you want.

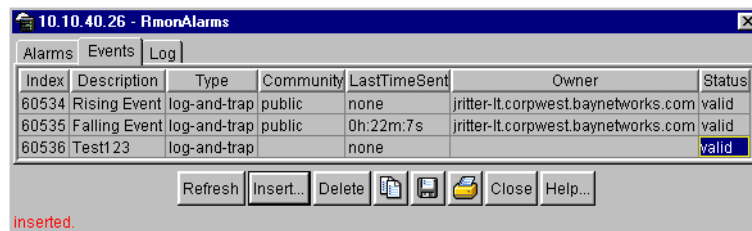
You can set the event type to log to save memory or to snmp-trap to reduce traffic from the switch or for better CPU utilization.

If you select snmp-trap or log-and-trap, you must set trap receivers.

- 4 Click Insert.

The new event is displayed in the Events tab (Figure 83).

**Figure 83** New event in the Events tab



Index	Description	Type	Community	LastTimeSent	Owner	Status
60534	Rising Event	log-and-trap	public	none	jritter-it.corpwest.baynetworks.com	valid
60535	Falling Event	log-and-trap	public	0h:22m:7s	jritter-it.corpwest.baynetworks.com	valid
60536	Test123	log-and-trap		none		valid

## Deleting an event

To delete an event:

- 1 In the Events tab, highlight an event Description.
- 2 Click Delete.

The event is removed from the table.

## Log information

The Log tab chronicles and describes the alarm activity, which is then generated to viewed.

To view the Log tab:

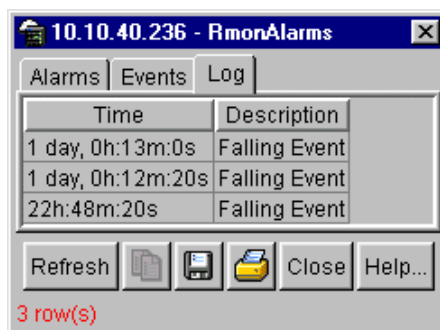
- 1 From the Device Manager main menu, choose RMON > Alarms.

The RMONAlarm dialog box opens with the Alarms tab displayed ([Figure 80 on page 163](#)).

- 2 Click the Log tab.

The Log tab opens ([Figure 84](#)).

**Figure 84** Log tab





---

Table 62 describes the Log tab fields.

**Table 62** Log tab fields

Item	Description
Time	An implementation-dependent description of the event that activated the log entry.
Description	Specifies whether the event is a rising or falling event.



---

## Chapter 9

# Security parameters

---

You can set the security features for a switch so that the actions are performed by the software when a violation occurs. The security actions you specify are applied to all ports of the switch.

This chapter describes the Security information available in Device Manager on the following tabs:

- General tab (next)
- AuthConfig tab ([page 176](#))
- SecurityList tab ([page 179](#))
- AuthStatus tab ([page 179](#))
- AuthViolation ([page 181](#))
- SSH ([page 183](#))
- SSH Sessions ([page 184](#))

## General tab

The General tab allows you to set and view general security information for the switch.

To view the General tab:

- ➡ From the Device Manager menu bar, select Edit > Security.

The Security dialog box opens with the General tab displayed ([Figure 85](#)).

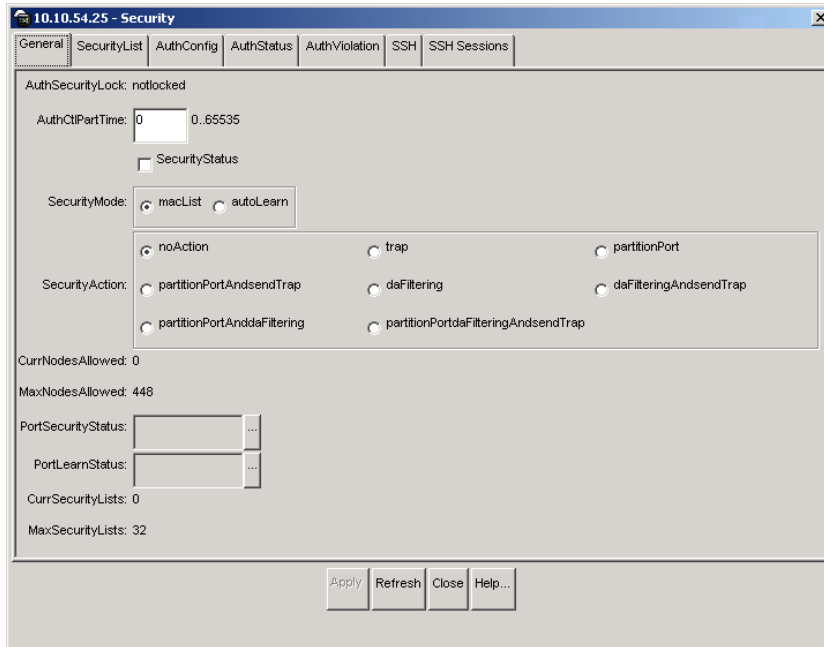
**Figure 85** General tab

Table 63 describes the General tab items.

**Table 63** General tab items

Items	Description
AuthSecurityLock	If this parameter is listed as “locked,” the agent refuses all requests to modify the security configuration. Entries also include: <ul style="list-style-type: none"> <li>• other</li> <li>• notlocked</li> </ul>
AuthCtlPartTime	This value indicates the duration of the time for port partitioning in seconds. Default: 0 (zero). When the value is zero, port remains partitioned until it is manually re-enabled.
SecurityStatus	Indicates whether or not the switch security feature is enabled.

**Table 63** General tab items (continued)

Items	Description
SecurityMode	<p>Mode of switch security. Entries include:</p> <ul style="list-style-type: none"> <li>• macList: Indicates that the switch is in the MAC-list mode. You can configure more than one MAC address per port.</li> <li>• autoLearn: Indicates that the switch learns the first MAC address on each port as an allowed address of that port.</li> </ul>
SecurityAction	<p>Actions performed by the software when a violation occurs (when SecurityStatus is enabled). The security action specified here applies to all ports of the switch.</p> <p>A blocked address causes the port to be partitioned when unauthorized access is attempted. Selections include:</p> <ul style="list-style-type: none"> <li>• noAction: Port does not have any security assigned to it, or the security feature is turned off.</li> <li>• trap: Listed trap.</li> <li>• partitionPort: Port is partitioned.</li> <li>• partitionPortAndsendTrap: Port is partitioned and traps are sent to the trap receiver.</li> <li>• daFiltering: Port filters out the frames where the destination address field is the MAC address of unauthorized Station.</li> <li>• daFilteringAndsendTrap: Port filters out the frames where the destination address field is the MAC address of unauthorized station. Traps are sent to trap receiver(s).</li> <li>• partitionPortAnddaFiltering: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station.</li> <li>• partitionPortdaFilteringAndsendTrap: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receiver(s).</li> </ul> <p><b>Note:</b> “da” means destination address.</p>
CurrNodesAllowed	Current number of entries of the nodes allowed in the AuthConfig tab.
MaxNodesAllowed	Maximum number of entries of the nodes allowed in the AuthConfig tab.
PortLearnStatus	Set of ports where auto-learning is enabled.
CurrSecurityLists	Current number of entries of the Security listed in the SecurityList tab
MaxSecurityLists	Maximum entries of the Security listed in the SecurityList tab.

## SecurityList tab

The SecurityList tab contains a list of Security port items.

To view the SecurityList tab:

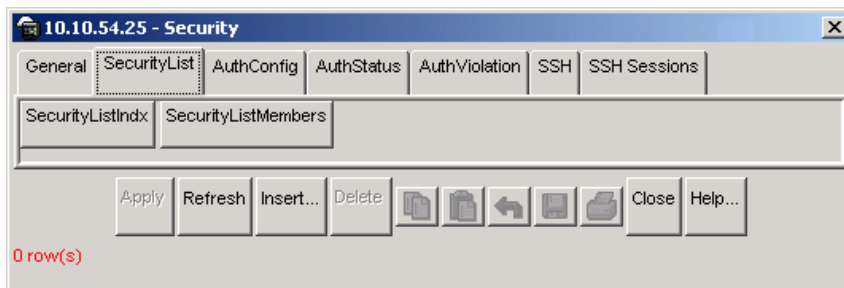
- 1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed ([Figure 85 on page 172](#)).

- 2 Click the SecurityList tab.

The SecurityList tab opens ([Figure 86](#)).

**Figure 86** SecurityList tab



[Table 64](#) describes the SecurityList tab fields.

**Table 64** SecurityList tab fields

Field	Description
SecurityListIdx	An index of the security list. This corresponds to the Security port list that can be used as an index into AuthConfig tab.
SecurityListMembers	The set of ports that are currently members in the Port list.

## Security, Insert SecurityList dialog box

Security, Insert SecurityList dialog box has editable fields for the SecurityList tab. Each row in this dialog box has information that can be updated or changed.

To view the Security, Insert AuthConfig dialog box:

- 1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed ([Figure 85 on page 172](#)).

- 2 Click the SecurityList tab.

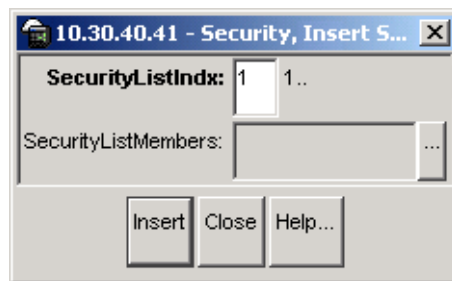
The SecurityList tab opens ([Figure 86 on page 174](#)).

- 3 Click inside a row.

- 4 Click Insert.

The Security, Insert SecurityList dialog box opens ([Figure 87](#)).

**Figure 87** Security, Insert SecurityList dialog box



[Table 65](#) describes the Security, Insert AuthConfig dialog box items.

**Table 65** Security, Insert AuthConfig dialog box fields

Field	Description
SecurityListIdx	An index of the security list. This corresponds to the Security port list that can be used as an index into AuthConfig tab.
SecurityListMembers	The set of ports that are currently members in the Port list.

## AuthConfig tab

The AuthConfig tab contains a list of boards, ports and MAC addresses that have the security configuration. An SNMP SET PDU for a row in the tab requires the entire sequence of the MIB objects in each entry to be stored in one PDU. Otherwise, GENERR return-value is returned.

To view the AuthConfig tab:

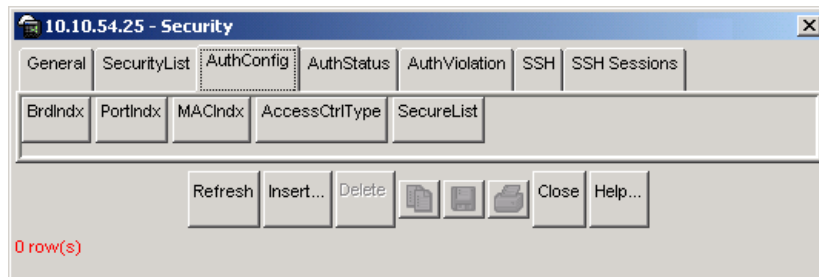
- 1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed ([Figure 85 on page 172](#)).

- 2 Click the AuthConfig tab.

The AuthConfig tab opens ([Figure 92](#)).

**Figure 88** AuthConfig tab



[Table 66](#) describes the AuthConfig tab fields.

**Table 66** AuthConfig tab fields

Field	Description
BrdIndx	Index of the slot containing the board on where the port is located. If you specify SecureList, this field must be 0.
PortIndx	Index of the port on the board. If you specify SecureList, this field must be 0.
MACIndx	An index of MAC addresses that are designated as allowed (station).



**Table 66** AuthConfig tab fields (continued)

Field	Description
AccessCtrlType	Displays the node entry as <code>node allowed</code> . A MAC address may be allowed on multiple ports.
SecureList	The index of the security list. This value is meaningful only if BrdIdx and PortIdx values are set to zero. For other board and port index values, it should also have the value of zero. The corresponding MAC Address of this entry is allowed or blocked on all ports of that this port list.

## Security, Insert AuthConfig dialog box

Security, Insert AuthConfig dialog box has editable fields for the AuthConfig tab. Each row in this dialog box has information that can be updated or changed.

To view the Security, Insert AuthConfig dialog box:

- 1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed ([Figure 85 on page 172](#)).

- 2 Click the AuthConfig tab.

The AuthConfig tab opens ([Figure 92 on page 183](#)).

- 3 Click inside a row.

- 4 Click Insert.

The Security, Insert AuthConfig dialog box opens ([Figure 89](#)).

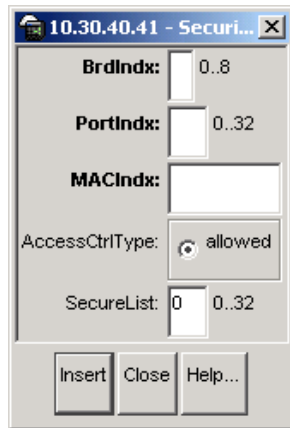
**Figure 89** Security, Insert AuthConfig dialog box

Table 67 describes the Security, Insert AuthConfig dialog box fields.

**Table 67** Security, Insert AuthConfig dialog box fields

Item	Description
BrdIdx	Index of the board. This corresponds to the index of the unit containing the board, but only if the index is greater than zero. A zero index is a wild card.
PortIdx	Index of the port on the board. This corresponds to the index of the last manageable port on the board, but only if the index is greater than zero. A zero index is a wild card.
MACIdx	An index of MAC addresses that are either designated as allowed (station) or not-allowed (station).
AccessCtrlType	Displays whether the node entry is node allowed or node blocked. A MAC address may be allowed on multiple ports.
SecureList	The index of the security list. This value is meaningful only if BrdIdx and PortIdx values are set to zero. For other board and port index values, it should also have the value of zero. The corresponding MAC Address of this entry is allowed or blocked on all ports of that this port list.

## AuthStatus tab

The AuthStatus tab displays information of the authorized boards and port status data collection. Information includes actions to be performed when an unauthorized station is detected and the current security status of a port. An entries in this tab may include:

- A single MAC address
- All MAC addresses on a single port
- A single port
- All the ports on a single board
- A particular port on all the boards
- All the ports on all the boards.

To view the AuthStatus tab:

- 1** From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed ([Figure 85 on page 172](#)).

- 2** Click the AuthStatus tab.

The AuthStatus tab opens ([Figure 90](#)).

Figure 90 AuthStatus tab

AuthStatusBrdIdx	AuthStatusPortIdx	AuthStatusMACIdx	CurrentAccessCtrlType	CurrentActionMode	CurrentPortSecurStatus
2	1	000000000000	allow	noAction	notApplicable
2	2	000000000000	allow	noAction	notApplicable
2	3	000000000000	allow	noAction	notApplicable
2	4	000000000000	allow	noAction	notApplicable
2	5	000000000000	allow	noAction	notApplicable
2	6	000000000000	allow	noAction	notApplicable
2	7	000000000000	allow	noAction	notApplicable
2	8	000000000000	allow	noAction	notApplicable
2	9	000000000000	allow	noAction	notApplicable
2	10	000000000000	allow	noAction	notApplicable
2	11	000000000000	allow	noAction	notApplicable
2	12	000000000000	allow	noAction	notApplicable
2	13	000000000000	allow	noAction	notApplicable
2	14	000000000000	allow	noAction	notApplicable
2	15	000000000000	allow	noAction	notApplicable
2	16	000000000000	allow	noAction	notApplicable
2	17	000000000000	allow	noAction	notApplicable
2	18	000000000000	allow	noAction	notApplicable
2	19	000000000000	allow	noAction	notApplicable
2	20	000000000000	allow	noAction	notApplicable
2	21	000000000000	allow	noAction	notApplicable
2	22	000000000000	allow	noAction	notApplicable
2	23	000000000000	allow	noAction	notApplicable
2	24	000000000000	allow	noAction	notApplicable
2	25	000000000000	allow	noAction	notApplicable
2	26	000000000000	allow	noAction	notApplicable

Table 68 describes the AuthStatus tab fields.

Table 68 AuthStatus tab fields

Item	Description
AuthStatusBrdIdx	The index of the board. This corresponds to the index of the slot containing the board if the index is greater than zero.
AuthStatusPortIdx	The index of the port on the board. This corresponds to the index of the last manageable port on the board if the index is greater than zero.
AuthStatusMACIdx	The index of MAC address on the port. This corresponds to the index of the MAC address on the port if the index is greater than zero.
CurrentAccessCtrlType	Displays whether the node entry is node allowed or node blocked type.

**Table 68** AuthStatus tab fields (continued)

Item	Description
CurrentActionMode	<p>A value representing the type of information contained, including:</p> <p>noAction: Port does not have any security assigned to it, or the security feature is turned off.</p> <p>partitionPort: Port is partitioned.</p> <p>partitionPortAndsendTrap: Port is partitioned and traps are sent to the trap receiver.</p> <p>Filtering: Port filters out the frames, where the destination address field is the MAC address of unauthorized station.</p> <p>FilteringAndsendTrap: Port filters out the frames, where the destination address field is the MAC address of unauthorized station. Trap are sent to trap receiver.</p> <p>sendTrap: A trap is sent to trap receiver(s).</p> <p>partitionPortAnddaFiltering: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station.</p> <p>partitionPortdaFilteringAndsendTrap: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receiver(s).</p>
CurrentPortSecurStatus	<p>Displays the security status of the current port, including:</p> <ul style="list-style-type: none"> <li>• If the port is disabled, notApplicable is returned.</li> <li>• If the port is in a normal state, portSecure is returned.</li> <li>• If the port is partitioned, portPartition is returned.</li> </ul>

## AuthViolation tab

The AuthViolation tab contains a list of boards and ports where network access violations have occurred, and also the identity of the offending MAC addresses.

To view the AuthViolation tab:

- 1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed ([Figure 85 on page 172](#)).

- 2 Click the AuthViolation tab.
- The AuthViolation tab opens (Figure 91).

Figure 91 AuthViolation tab

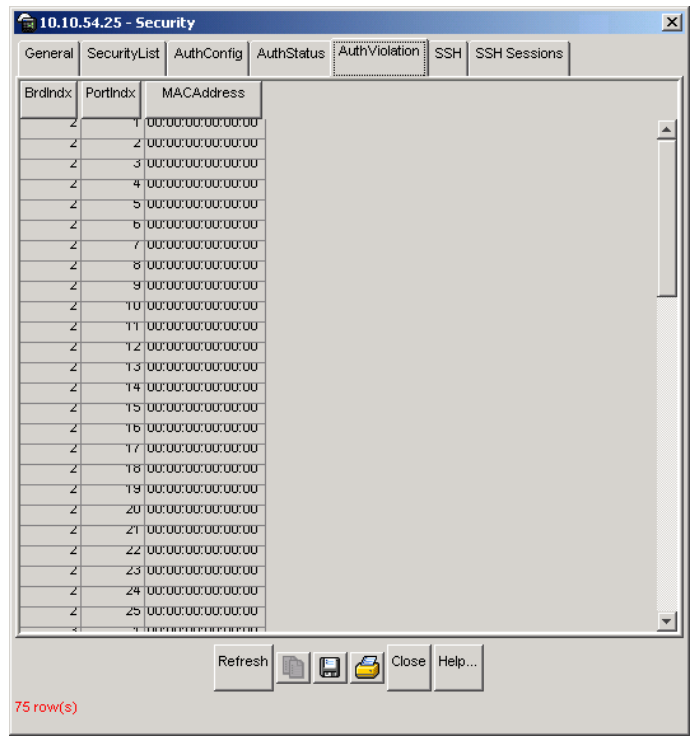


Table 69 describes fields for the AuthViolation tab fields.

Table 69 AuthViolation tab fields

Field	Description
BrdIndx	The index of the board. This corresponds to the unit containing the board. The index will be 1 where it is not applicable.
PortIndx	The index of the port on the board. This corresponds to the port on that a security violation was seen.
MACAddress	The MAC address of the device attempting unauthorized network access (MAC address-based security).

# SSH tab

The SSH tab displays the parameters available for SSH.

To view the SSH tab:

- 1 From the Device Manager menu bar, select Edit > Security.  
The Security window opens with the General tab displayed (Figure 85 on page 172).
- 2 Click the SSH tab.  
The SSH tab opens (Figure 92).

Figure 92 SSH tab

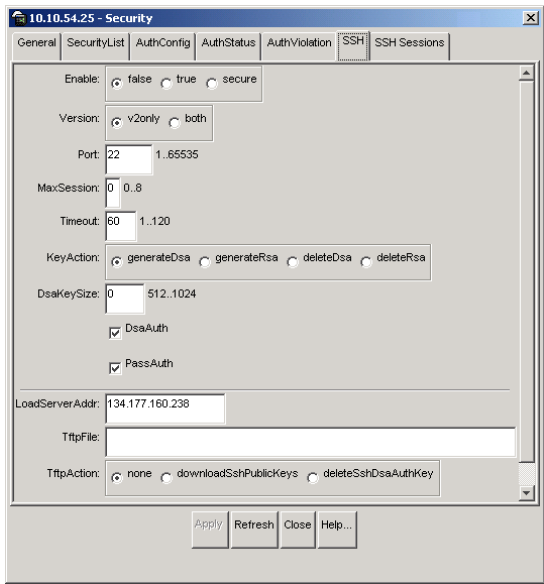


Table 70 describes the SSH tab fields.

Table 70 SSH tab fields

Field	Description
Enable	
Version	

**Table 70** SSH tab fields (continued)

Field	Description
Port	
Maxsession	
Timeout	
KeyAction	
DsaKeySize	
DsaAuth	
PathAuth	
LoadServerAddr	
TftpFile	
TftpAction	
TftpResult	

## SSH Sessions tab

The SSH Sessions tab displays the currently active SSH sessions.

To view the SSH Sessions tab:

- 1 From the Device Manager menu bar, select Edit > Security.  
The Security window opens with the General tab displayed ([Figure 85 on page 172](#)).
- 2 Click the SSH Sessions tab.  
The SSH Sessions tab opens ([Figure 92](#)).



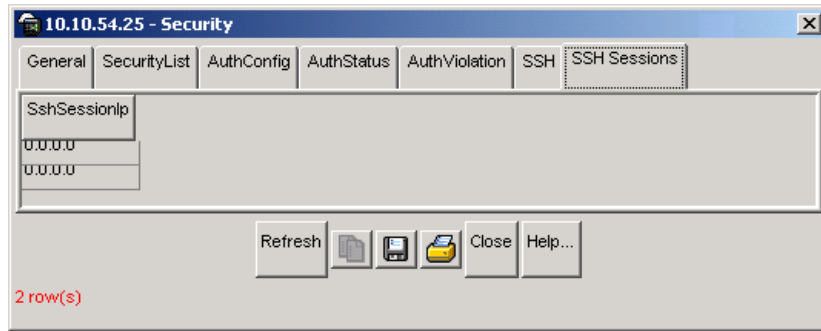
**Figure 93** SSH Sessions tab

Table 70 describes the SSH Sessions tab fields.

**Table 71** SSH Sessions tab fields

Field	Description
SSHSessions	Lists the currently active SSH sessions.



# Index

---

## Symbols

[<=64 field 113](#)  
[>1023 field 114](#)  
[>127 field 113](#)  
[>255 field 113](#)  
[>511 field 114](#)  
[>64 field 113](#)

## A

[AbsoluteValue statistics 39](#)  
[access levels 27](#)  
[Action field 72](#)  
[Actions menu 30](#)  
[ActiveMember field 126](#)  
[ActiveMembers field 130](#)  
[Addr field 53](#)  
[AddrMaskReps field 81, 83](#)  
[AddrMasks field 81, 83](#)  
[AdminControlledDirections field 95, 102](#)  
[AdminDuplex field 88, 99](#)  
[AdminSpeed field 88, 99](#)  
[AdminState field 61](#)  
[AdminStatus field 87, 98](#)  
[Agent Info tab 63](#)  
[Alarm Manager button 31](#)  
[alarms tab 163, 164](#)  
[alarms, RMON](#)  
     [characteristics of 157](#)  
     [creating 159](#)

[AlignmentErrors field 108, 122](#)  
[Area Chart button 45](#)  
[area graph example 40](#)  
[ARP tab 54](#)  
[AuthConfig tab](#)  
     [AccessCtrlType field 177](#)  
     [BrdIndx field 176](#)  
     [MACIndx field 176](#)  
     [PortIndx field 176](#)  
     [SecureList field 177](#)  
[AuthControlledPortControl field 95, 102](#)  
[AuthControlledPortStatus field 95, 102](#)  
[AuthenticationTraps field 57](#)  
[AuthStatus tab](#)  
     [AuthStatusBrdIndx field 180](#)  
     [AuthStatusMACIndx field 180](#)  
     [AuthStatusPortIndx field 180](#)  
     [CurrentAccessCtrlType field 180](#)  
     [CurrentActionMode field 181](#)  
     [CurrentPortSecurStatus field 181](#)  
[AuthViolation tab](#)  
     [BrdIndx field 182](#)  
     [MACIndx field 182](#)  
     [PortIndx field 182](#)  
[AutoNegotiate field 88, 99](#)  
[Average statistics 39](#)

## B

[BackendAuthState field 95, 102](#)  
[Bar Chart button 45](#)  
[Base tab 131](#)  
[BcastAddr field 53](#)

- blinking LEDs 34
- BootMode field 57
- BootRouterAddr tab 63
- Bridge dialog box 131
- Bridge parameter
  - Base tab
    - BridgeAddress field 132
    - NumPorts field 132
    - Type 132
  - Forwarding tab
    - Address field 138
    - Port field 138
    - Status field 138
  - Spanning Tree tab
    - BridgeHelloTime field 135
    - BridgeMaxAge field 134
    - DesignatedRoot field 133
    - ForwardDelay field 134
    - HelloTime field 134
    - MaxAge field 134
    - Priority field 133
    - ProtocolSpecification field 133
    - RootCost field 134
    - RootPort field 134
    - TimeSinceTopologyChange field 135
    - TimeSinceTopologyChange field 133
    - TopChanges field 133
  - Transparent tab
    - AgingTime field 136
    - LearnedEntryDiscard field 136
- BroadcastPkts field 112
- buckets 150
- BucketsGranted field 153
- BucketsRequested field 153
- buttons
  - dialog boxes 37
  - toolbar 31

## C

- CarrierSenseErrors field 108, 122
- chassis

- configuration, editing 55
  - graphing 74
- Chassis ICMP In statistics window 80
- Chassis ICMP Out statistics tab 82
- Chassis SNMP tab 75
- Collisions field 113
- Color field 126
- color-coded ports 34
- communication parameters, setting for Device Manager 24
- Community field 66, 166
- community strings
  - default 27
  - entering 28
- ConfigFileName field 71, 73
- configuration
  - downloading 70
  - Multi-Link Trunks 118
  - port-based VLAN 126, 127
  - ports 145
- Confirm row deletion field 26
- Control tab 152
- conventions, text 19
- Copy button 37
- Copy File tab 70
- CRAAlignErrors field 113
- Cumulative statistics 39
- CurrentDefaultGateway field 57
- CurrentImageVersion field 57
- CurrentMgmtProtocol field 57
- customer support 21

## D

- data, exporting 43
- default access community strings 27
- Default TTL field 52
- DefaultVLANId field 90, 101

DeferredTransmissions field 109, 123  
 Descr field 59, 61, 68, 70, 87, 98  
 Description field 166  
 DestUnreachs field 81, 83  
 Device Manager  
     setting properties 24  
 Device Manager window 23, 24  
 Device menu 30  
 Device Name field 28  
 device view, summary 31  
 device, opening 27  
 Disable command 36  
 disabled port, color 35  
 DiscardUntaggedFrames field 90, 101

## E

EapLengthErrorFramesRx field 115  
 EAPOL 93, 114, 116  
 EAPOL Diag tab 116  
 EAPOL Stats tab 114  
 EAPOL tab for multiple ports 101  
 EapolFramesRx field 115  
 EapolFramesTx Field 115  
 EapolLogoffFramesRx field 115  
 EapolReqFramesTx field 115  
 EapolReqIdFramesTx field 115  
 EapolRespFramesRx field 115  
 EapolRespldFramesRx 115  
 EapolStartFramesRx field 115  
 EchoReps field 81, 83  
 Echos field 81, 83  
 Edit command 36  
 Edit menu 30  
 Edit Selected button 31  
 Enable command 36

Enable field 26  
 Ether Stats Control tab 155  
 Ethernet Errors tab 107  
 Ethernet statistics, disabling 156  
 Event Index field 162  
 events, RMON 165  
 ExcessiveCollisions field 109, 123  
 Export Data button 37, 43

## F

falling event 165  
 falling value, RMON alarms 157  
 FallingEventIndex field 164  
 FallingThreshold field 164  
 Fan tab 69  
 FCSErrors field 108, 122  
 File System window 70  
 Forwarding tab 136  
 ForwDatagrams field 79  
 FragCreates field 79  
 FragFails field 79  
 FragOKs field 79  
 frames, discarding tagged frames on 129  
 FrameTooLongs field 109, 123

## G

Globals tab 52  
 graph  
     creating 43  
     modifying 44  
 Graph command 36  
 graph dialog box 44  
 Graph menu 30  
 Graph Selected button 31, 43  
 graph types 39  
 graphPort, Interface tab 104

## H

Help button 31  
Help menu 30  
Help, Device Manager 49  
Horizontal button 45

## I

ICMP In tab 81  
ICMP Out statistics 82  
ICMP Out tab 82  
ifInNUcastPkts field 105  
ifInOctets field 105  
ifInUcastPkts field 105  
ifOutNUcastPkts field 105  
ifOutOctets field 105  
ifOutUcastPkts field 105  
image file 70  
ImageFileName field 63, 71, 73  
ImageLoadMode field 57  
InAddrErrors field 78  
InASNParseErrs field 76  
InBadCommunityNames field 76  
InBadCommunityUses field 76  
InBadValues field 76  
InBadVersions field 76  
InBroadcastPkt field 120  
InDelivers field 79  
Index field 87, 98, 102, 162  
InDiscards field 79, 105  
InErrors field 105  
InGenErrs field 77  
InGetNexts field 76  
InGetRequests field 76  
InGetResponses field 76  
InHdrErrors field 78  
InMulticastPkts field 120  
InNoSuchNames field 76  
Inpkts field 75  
InReadOnlys field 77  
InReceives field 78  
Insert Alarm dialog box 160  
Insert AuthConfig dialog box  
    BrdIndx field 178  
Insert button 37  
Insert Control dialog box 153  
Insert Ether Stats dialog box 156  
Insert Event dialog box 167  
InSetRequests field 76  
Interface item, ARP 54  
Interface tab 86  
Interface tab for a multiple port 97  
Interface window 120  
InternalMacReceiveErrors field 108, 122  
InternalMacTransmitErrors field 108, 122  
Interval field 153, 163  
InTooBigs field 76  
InTotalReqVars field 75  
InTotalSetVars field 75  
InUnknownProtos field 79, 106  
InvalidEapolFramesRx field 115  
IP Address tab 53  
IP dialog box 51  
IP tab 78  
IPAddress field 54

## J

Jabbers field 113

## K

KeyTxEnabled field 95, 103

**L**

LastChange field 88, 99  
LastEapolFrameSource 95  
LastEapolFrameSource field 103  
LastEapolFrameVersion field 95, 103  
LastLoadProtocol field 58  
LastTimeSent field 166  
LastUnauthenticatedCommunityString field 65  
LastUnauthenticatedIpAddress field 65  
LastValue statistics 39  
LateCollisions field 109, 123  
LEDs in device view 34  
legend, port color 30, 35  
Line Chart button 45  
link, lacking, color 35  
LoadServerAddr field 63, 71, 73  
LocalStorageImageVersion field 57  
Location field 59, 61  
Log Scale button 45  
Log tab 168  
logs 168  
LstChng field 59, 61

**M**

MacAddr field 63  
MacAddress field 54  
Max Traps in Log field 26  
Maximum statistics 39  
MaxReq field 95, 103  
MDA  
    viewing 33  
menu bar, Device Manager 30  
menus. *See* individual menu names  
Minimum statistics 39  
MLT requirements 117

MltId field 88, 99  
Mtu field 87, 98  
MulticastPkts field 113  
Multi-Link Trunk window 119  
Multi-Link Trunking. *See* MLT  
Multi-Link Trunks window 118  
multiple objects, selecting 33  
MultipleCollisionFrames field 109, 123

**N**

Name field 118, 126  
NetMask field 53  
new table entry, creating 37  
NextBootDefaultGateway field 57  
NextBootLoadProtocol field 58  
NextBootMgmtProtocol field 57  
NextBootNetMask field 63  
NextBootpAddr field 63  
NmmCurNum field 146  
NmmLstChg field 146  
NmmMaxNum field 146  
NoSuchObject error message 85, 96

**O**

object types 32  
objects  
    editing 38  
    selecting 32  
Octets field 112  
online Help 30, 49  
Open Device button 27, 31  
Open Device dialog box 27, 28, 30  
operating port, color 34  
OperControlledDirections field 95, 102  
OperSpeed field 88, 99  
OperState field 62, 68, 70

OperStatus field 88, 99  
OutBadValues field 76  
OutBroadcast field 120  
OutDiscards field 79, 105  
OutErrors field 106  
OutGenErrs field 76  
OutMulticast field 120  
OutNoRoutes field 79  
OutNoSuchNames field 76  
Outpkts field 75  
OutRequests field 79  
OutTooBigs field 76  
OutTraps field 76  
OversizePkts field 113  
Owner field 153, 155, 164, 166

## P

PaeState 94  
PaeState field 102  
ParmProbs field 81, 83  
Paste button 37  
PhysAddress field 87, 98  
Pkts field 112  
polling interval 43  
Port Capabilities field 94  
port color legend 35  
Port dialog box 104  
port Ethernet Error Statistics tab 106  
Port field 155  
Port Interface tab 86, 98  
port shortcut menu 36  
Port Spanning Tree window 91  
PortCapabilities field 102  
PortInitialize field 94, 102  
PortMembers field 118, 126, 130

PortProtocolVersion field 94, 102  
PortReauthenticate field 94, 102

### ports

- color-coded 34
- configuring 85, 145
- controlling 85
- disabled 35
- editing 85, 95
- graphing 86, 97, 103, 104
- selecting 33
- viewing 85, 95

PortType field 118

Power Supply tab 68

Print button 37

product support 21

Properties dialog box 24, 25

- Hotswap Poll Interval field 26

- If Traps, Status Interval

- ) field 26

- Status Poll Interval field 26

publications

- related 20

## Q

QuietPeriod field 95, 102

## R

Read Community field 28

Read Community, SNMP 28

Read Community, SNMP field 28

Read-Write-All access 28

ReasmFails field 80

ReasmMaxSize field 53

ReasmOKs field 80

ReasmReqds field 79

ReasmTimeout field 52

ReAuthEnabled field 95, 103

ReAuthPeriod field 95, 103



- 
- Reboot field 58
  - Redirects field 81, 83
  - Refresh Device Status button 31
  - Register for Traps field 26
  - Remote Monitoring. *See* RMON
  - Reset Changes button 37
  - Result field 72
  - Retry Count field 26
  - rising event 165
  - rising value, RMON alarms 157
  - RisingEventIndex field 164
  - RisingThreshold field 164
  - RMON
    - alarms
      - characteristics 157
      - creating 159
      - deleting 163
      - inserting 161
    - events
      - definition 165
    - history
      - creating 152
      - definition 150
      - disabling 154
    - statistics 149, 152
  - RMON EtherStat tab 112, 150
  - RMON Event tab 166
  - Rmon menu 30
- S**
- Sample Interval field 162
  - Sample Type field 162, 163
  - security 93
  - Security parameters
    - General tab
      - AuthCtlPartTime field 172
      - AuthSecurityLock field 172
      - CurrNodesAllowed field 173
      - CurrSecurityLists field 173
      - MaxNodesAllowed field 173
      - MaxSecurityLists field 173
      - PortLearnStatus field 173
      - SecurityAction field 173
      - SecurityMode field 173
      - SecurityStatus field 172
  - Security, Insert AuthConfig dialog box
    - AccessCtrlType field 178
    - MACIndx field 178
    - PortIndx field 178
    - SecureList field 178
  - SerNum field 59, 62
  - ServerTimeout 103
  - ServerTimeout field 95
  - shortcut menus
    - port 36
    - switch unit 35
  - single object, selecting 32
  - SingleCollisionFrames field 109, 123
  - SNMP Info tab 64
  - SNMP tab 64
  - SNMP traps 47
  - Spanning Tree tab 132, 133
  - Spanning Tree window 91
  - Speed field 99
  - SQETestErrors field 109, 123
  - SrcQuenchs field 81, 83
  - Stack Info tab 60
  - Stacked button 45
  - Standalone Unit Info Tab 59
  - StartupAlarm field 164
  - statistics
    - Ethernet statistics, enabling 155
    - for a single object 42
    - for multiple objects 42
    - graphing 38
    - ICMP Out 82
    - MLT 119
    - RMON 149, 152
-

- single port 42
  - types 39
  - statistics dialog box
    - multiple objects 42
  - statistics dialog boxes 30
  - Status field 146, 164
  - STG 91
  - STG dialog box
    - Ports tab
      - DesignatedBridge field 144
      - DesignatedCost field 144
      - DesignatedPort field 144
      - DesignatedRoot field 144
      - EnableStp field 143
      - FastStart field 143
      - ForwardTransitions field 144
      - PathCost field 144
      - Priority field 143
      - State field 143
      - StgId field 143
  - StgId field 126, 130
  - Stop button 37
  - support, Nortel Networks 21
  - SuppTiemout field 103
  - SuppTimeout field 95
  - switch stack, selecting 33
  - switch unit shortcut menu 35
  - switch, selecting 32
  - sysContact field 56
  - sysDescr field 56
  - sysLocation field 56
  - sysName field 56
  - System tab 56
  - sysUpTime field 56
- T**
- tagged frame, discarding 129
  - technical support 21
  - Telnet button 31, 45
  - Telnet session 30, 31, 45
  - text conventions 19
  - Threshold Type field 162
  - TimeExcds field 81, 83
  - Timeout field 26
  - TimestampReps field 81, 83
  - Timestamps field 81, 83
  - toolbar, Device Manager 31
  - topology 145
  - Trace field 26
  - Transparent Bridging tab 110, 115, 116
  - Transparent tab 135
  - trap log 47
  - Trap Log button 31
  - Trap Port field 26
  - Trap Receivers
    - NetAddr field 66
  - Trap Receivers tab 65
  - troubleshooting
    - locations of Help files 49
    - receiving traps 47
  - TrpRcvrCurEnt field 65
  - TrpRcvrMaxEnt field 65
  - TrpRcvrNext field 65
  - TxPeriod field 95, 102
  - Type 126
  - Type field 54, 59, 87, 89, 98, 100, 166
  - types of objects 32
- U**
- UndersizePkts field 113
  - UNIX
    - receiving traps 47

## V

- ValidFlag tab 63
- Value field 162, 163
- value, changed 38
- Variable field 162, 163
- Ver field 59, 62
- Viewing 85
- VLAN 88
  - VLAN Basic tab 126, 127
  - VLAN dialog box 126, 127
  - VLAN menu 30
  - VLAN tab 89, 94
  - VLAN tab for multiple ports 99
- VlanIds field 89, 100
- VLANs
  - limitations 125
  - managing 130

## W

- Web-based management interface
  - home page, graphic 47
- window, Device Manager 29
- Write Community field 28
- Write Community, SNMP 28